

26.9.2018

Eduskunnan puolustusvaliokunnalle

*Vastine asiantuntijalausuntoihin***Hallituksen esitys siviilitiedustelua koskevaksi lainsäädännöksi (HE 202/2017 vp)****Sisällys**

1 Johdanto	2
2 Poliisilaki 5 a luku 44 § Siviilitiedustelussa saadun tiedon luovuttaminen rikostorjuntaan (ns. palomuuuri)	2
3 Siviilitiedustelun kohteet (Poliisilaki 5 a luku 3 § ja tietoliikennetiedustelulaki 3 §)	7
4 Salaisen tiedonhankinnan yhteensovittaminen (Poliisilaki 5 a luku 56 §)	10
5 Suojelupoliisin poliisius	11
6 Toimivaltuudet (Tiedustelumenetelmät)	12
6.1 Tietoliikennetiedustelun käytön edellytykset	12
6.2 Tietolähteen turvaaminen siviilitiedustelussa (Poliisilaki 5 a luku 25 §)	14
6.3 Paikkatiedustelun kohde	15
6.4 Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen (Poliisilaki 5 a luku 16 §)	15
6.5 Lupa-aika 6kk	16
6.6 Kansainvälinen yhteistyö	17
7 Tiedusteluvaltuutetun rooli tuomioistuimessa	18
8 Ilmoitus syyttäjälle poliisirikoksista	19
9 Kansallisen turvallisuuden käsite	20
10 Tiedustelumenetelmien käyttöalan laajentuminen suhteessa nykyisiin rikostorjuntatoimivaltuuksiin	21
11 Tietoliikennetiedustelun yleisen, kohdentamattoman ja kaiken kattavan seurannan kielto	25
12 Valtiollinen toimija	27
13 Viranomaisyhteistyö ja tietojen luovuttaminen	28
14 Teleyritysten kustannusten korvaaminen	29
15 Tiedustelumenetelmän käytöstä ilmoittaminen ja raportointi	31
16 Yrityssalaisuuden suoja	33
17 Ilmiantajan suoja (ns. whistleblower)	34
18 Henkilötietojen käsittely	34
19 Virkamiesten koulutus	34
20 Tuomioistuinmenettely	36
21 Ilmaisukielto	37
22 Vieraan valtion virkamies tiedustelumenetelmän käyttäjänä	37
23 Liitelait	38
23.1 Laki poliisin hallinnosta	38
24 Eräitä yhteensovittamisen tarpeita	38
24.1 Tietojenantovelvollisuus tietoliikennetiedustelussa	38
24.2 Tekninen laitetarkkailu	39

24.3	Tiedustelutoimivaltuuksien käyttö ulkomailla.....	40
------	---	----

1 Johdanto

Eduskunnan puolustusvaliokunta on pyytänyt sisäministeriöltä kirjallista vastinetta hallituksen esityksestä siviilitiedustelua koskevaksi lainsäädännöksi (HE 202/2017 vp) annettuihin asiantuntijalausuntoihin.

Pääsääntöisesti lakiesityksistä annettu palaute on ollut positiivista ja lausunnonantajat ovat pitäneet ehdotuksia hyvinä ja kannatettavina. Sisäministeriön näkemys on, että lausunnot eivät yleisesti ottaen anna suurta aihetta ehdotettujen pykälien muuttamiseen.

Pyydettyä vastineena asiantuntijalausunnoista sisäministeriö esittää lausuntokohtaisesti, siltä osin kuin lausunnot ovat edellyttäneet vastaamista, seuraavaa:

2 Poliisilaki 5 a luku 44 § Siviilitiedustelussa saadun tiedon luovuttaminen rikostorjuntaan (ns. palomuururi)

Eduskunnan oikeusasiamies pitää perusteltuna, että syyttömyyttä tukevan tiedon luovutuksen harkinnan perusteista säädettäisiin laissa. Lisäksi eduskunnan oikeusasiamies pitää tärkeänä, että ratkaisujen perusteet ja päätösmenettely siviilitiedustelulain 44 §:ssä ja sotilastiedustelulain 76 ja 77 §:ssä tarkoitetuissa tilanteissa dokumentoitaisiin jälkikäteiskontrollin mahdollistamiseksi.

Sisäministeriön vastaus: Poliisilain 5 a luvun 44 §:ssä ehdotetaan säädettäväksi niin sanotusta palomuurista. Tiedustelutoimivaltuuksilla saatuja tietoja ei lähtökohtaisesti saisi käyttää muuhun tarkoitukseen kuin kansallisen turvallisuuden suojaamiseksi. Palomuurissa säädettäisiin eräistä poikkeuksista käyttötarkoitussidonnaisuuteen.

Tiedustelumenetelmien käyttötarkoituksesta johtuen on selvää, että harkinnanvaraisissa rikostiedon luovuttamistapauksissa keskeinen arviointikriteeri on luovuttamisen vaikutus kansalliseen turvallisuuteen. Ilmoituksen lykkäämistilanteessa suojelupoliisin olisi kuitenkin suhteutettava toisiinsa yhtäältä kansallisen turvallisuuden taikka hengen tai terveyden suojaamisintressi ja toisaalta rikoksen selvittämisentressi.

Pykälän 4 momentin mukaan:

Tiedustelumenetelmän käytöllä saatua tietoa saa aina luovuttaa syyttömyyttä tukeväksi selvitykseksi sekä hengelle, terveydelle tai vapaudelle aiheutuvan merkittävän vaaran taikka huomattavan ympäristö-, omaisuus- tai varallisuusvahingon estämiseksi.

Kyseisen lainkohdan tulkintaa tulisivat ohjaamaan sen perustelut, voimassa oleva käytäntö sekä poliisioikeudelliset periaatteet. Lainkohdan perustelujen mukaan:

Esitutinnan tasapuolisuusperiaatteen sekä jokaiselle kuuluvan oikeuden oikeudenmukaiseen oikeudenkäyntiin ja henkilökohtaiseen vapauteen kannalta on selvää, että pyyntöön saada syyttömyyttä tukevaa selvitystä on suhtauduttava esitutkinnassa sitä vakavammin, mitä suurempi on vaara, että henkilö pidätetään, vangitaan tai hän joutuu muun pakkokeinon kohteeksi tai joutuu syytteeseen tai tuomitaan rangaistukseen tai muuhun rikosoikeudelliseen seuraamukseen virheellisin perustein. Samoihin seikkoihin on viran puolesta kiinnitettävä huomiota myös silloin, kun suojelupoliisi harkitsee oma-aloitteista tiedonluovuttamista syyttömän tueksi. Suojelupoliisin oma-aloitteinen tiedonluovutus syyttömän tueksi voisi tulla kyseeseen lähinnä 5 momentin mukaisissa tilanteissa eli silloin, kun esitutkintaviranomainen on ilmoittanut suojelupoliisille sen tiedonhankinnan kohteena ollutta tai edelleen olevaa henkilöä koskevan esitutkinnan käynnistämisestä, esitutkintatoimenpiteen käyttämisestä taikka rikoksen estämiseen tähtäävän toimenpiteen käynnistämistä. Epäillyn pyyntö puolestaan voisi käytännössä tulla kyseeseen vain silloin, kun hän on saanut ilmoituksen tiedustelumenetelmän käytöstä.

Pykälän 4 momentti perustuu hyvin pitkälle voimassa olevan poliisilain 5 luvun 54 §:n 4 ja 5 momenttiin, joiden mukaan:

Ylimääräistä tietoa saa lisäksi käyttää aina rikoksen estämiseksi, poliisin toiminnan suuntaamiseksi ja syyttömyyttä tukevana selvityksenä.

Ylimääräistä tietoa saa käyttää myös hengelle, terveydelle tai vapaudelle aiheutuvan merkittävän vaaran taikka huomattavan ympäristö-, omaisuus- tai varallisuusvahingon estämiseksi.

Kyse olisi vastaavantyypisistä tiedon luovuttamisesta siltä osin kuin kyse on tiedon luovuttamisesta syyttömyyttä tukevaksi selvitykseksi sekä hengelle, terveydelle tai vapaudelle aiheutuvan merkittävän vaaran taikka huomattavan ympäristö-, omaisuus- tai varallisuusvahingon estämiseksi, mitä nykyisin poliisilain 5 luvun 54 §:n 4 ja 5 momentin ja pakkokeinolain 10 luvun 56 §:n 4 ja 5 momentissa säädetään.

Puolustusasianajajat tekevät jo nykyisin suojelupoliisille tietopyyntöjä, jotka koskevat sellaisia poliisilain 5 luvun nojalla käytettyjä salaisia tiedonhankintakeinoja, joiden käyttäminen on johtanut esitutkinnan käynnistymiseen. Asianosaisella on esitutkinnan aloittamisen jälkeen oikeus saada tieto esitutkintaan johtaneista ja esitutkinnassa ilmi tulleista seikoista sekä esitutkinta-aineistosta, joka voi tai on voinut vaikuttaa hänen asiansa käsittelyyn (esitutkintalain 4 luvun 15 §:n 1 momentti). Korkeimman oikeuden ratkaisussa KKO 2011:27 määrittelemiä linjauksia ei ole tämän lainsäädännön yhteydessä tarkoitus muuttaa.

On sinänsä ymmärrettävää, että usea lausunnonantaja näkee suojelupoliisin tiedustelumenetelmien tiedonhankinnan ikään kuin jatkumona rikostorjuntamenetelmien käyttämiseen. Tässä yhteydessä on tarpeen painottaa, ettei tiedustelumenetelmien käytön pääasiallinen tarkoitus ole rikostiedon hankkiminen, vaan tiedon hankkiminen siviilitiedustelun kohteena olevasta toiminnasta, joka muodostaa vakavan uhkan Suomen kansalliselle turvallisuudelle.

Lakiehdotuksen 5 a luvun 62 §:ssä säädettäisiin asetuksenantovaltuuksista. Pykälän 1 momentin 4 kohdassa ehdotetaan säädettäväksi rikostorjuntaan luovutettavan tiedon siirtämistä koskevasta menettelystä. Tämä koskee myös ratkaisujen perusteiden ja päätösmenettelyn dokumentointia koskevaa menettelyä jälkikäteiskontrollin mahdollistamiseksi.

Poliisihallitus toteaa, että ehdotetun säännöksen mukaan lykkäyspäätöksen tekisi suojelupoliisi yksin ilman kolmansien etukäteiskontrollia tai keskustelua. Poliisihallitus katsoo, että käyttöperusteen syytä olla tarkoituksenmukaisesti kapea ja tarkkarajainen. Nyt pykälässä käytetty käsite "kansallinen turvallisuus" ei lienekään ympäröivänä riittävän tarkkarajainen siirtämisen peruste. Kansallinen turvallisuus tulisi poistaa ja muuttaa säännöstä siten, että siirtäminen olisi mahdollista vain, jos ilmoittamisesta aiheutuisi "vakavaa vahinkoa Suomen diplomaattisille suhteille tai muille elintärkeille eduille".

Helsingin poliisilaitos katsoo, että vuoden mittaisen lykkäyspäätöksen määräaikaa itsessäänkin on pidettävä melko pitkänä ottaen huomioon, että kyseessä ovat vakavat rikokset ja niiden selvittämisintressi on suuri niin yleisen kuin yksityisen edun kannalta. Suojelupoliisin tiedustelussa esiin tulleet rikoksentehtäjät ovat todennäköisesti suunnitelleet rikoksensa ja vuoden viive ilmoittamisessa tekee käytännössä ilmoittamisen merkityksettömäksi sen vuoksi, että tässä ajassa todistusaineisto on ehditty hävittää, epäillyt ovat poistuneet maasta, todistajien muistikuvat ovat heikentyneet eikä esim. telepakkokeinoilla ole enää mahdollisuutta saada tietoja teletointayritysten tiedon säilytysaikaan koskevien säännösten vuoksi (laki sähköisen viestinnän palveluista 157 §).

Lykkäyspäätöksen tekisi ehdotetun säännöksen mukaan suojelupoliisin päällikkö yksin ilman tuomioistuinkontrollia tai keskustelua KRP:n edustajan kanssa. Vertailun vuoksi todettakoon, että poliisin käytäessä salaisia tiedonhankintakeinoja ja halutessaan lykätä ilmoittamista asiasta tiedonhankinnan kohteelle, päättää asiasta tuomioistuin poliisin esityksestä (poliisilaki 5 luku 58 §, pakkokeinolaki 10 luku 60 §).

Suojelupoliisi ei nykyisinkään suorita juuri esitutkintaa ja esitutkintavaltuuksien kokonaan poistuessa voidaan kyseenalaistaa sen kompetenssin riittävyys arvioida esitutkintakynnyksen täyttymistä eri tunnusmerkistöjen osalta.

Myös **Keskusrikospoliisi** on kiinnittänyt huomiota, että mikäli asiassa päädytään rakenteeseen, jossa päätöksen tekee suojelupoliisin päällikkö itsenäisesti, tulee käytännössä esimerkiksi yhteistyövelvoitteen kautta varmistaa, että hänellä on riittävät tiedot intressipunninnan suorittamiseksi. Yhteistyövelvoite poliisin kanssa ei ole uusi asia, vaan viranomaisen väliseen yhteistyöhön velvoittava säännös löytyy jo nykyisin laista rikostorjunnasta Rajavartiolaitoksessa (7 §), laista rikostorjunnasta

Tullissa (2:2 §) ja laista sotilaskurinpidosta ja rikos-torjunnasta puolustusvoimissa (40 §). Eduskunta on siis aikaisemmin linjannut, että poliisi on yleisviranomainen rikostorjunta-asioissa.

Sisäministeriön vastaus: Poliisihallituksen, Helsingin poliisilaitoksen ja keskusrikospoliisin huomioid kohdistuvat pykälän 1 momenttiin, jonka mukaan suojelupoliisin päällikön päätöksellä keskusrikospoliisille tehtävää ilmoitusta ns. ylitörkeästä rikoksesta voitaisiin siirtää enintään vuodeksi kerrallaan, jos se on välttämätöntä kansallisen turvallisuuden varmistamiseksi tai hengen tai terveyden suojaamiseksi. Lainsäädäntöteknisesti vastaavantyyppinen konstruktio on poliisilain 5 luvun 58 §:n 2 momentissa (myös pakkokeinolain 10 luvun 60 §:n 3 momentissa), jonka mukaan tiedonhankinnan kohteelle tehtävä ilmoitus saadaan tuomioistuimen päätöksellä jättää kokonaan tekemättä, jos se on välttämätöntä valtion turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi.

Erona luonnollisesti on, että palomuurissa asiallisesti kyse on siviilitiedustelussa tiedustelumenetelmällä saadun rikostiedon ilmoittamisesta ja luovuttamisesta keskusrikospoliisille, kun edellä tarkoitettussa pykälässä salaisen tiedonhankintakeinon käytön ilmoittamisesta sen kohteelle. Näin ollen kyseisiä säännöksiä ei ole mahdollista täysin verrata toisiinsa. Todettakoon, että "kansallisen turvallisuuden varmistaminen" on merkityssisällöltään laajempi kuin Poliisihallituksen ehdottama Suomen diplomaattiset suhteet ja muut elintärkeät edut, ja näin ollen lähempänä valtion turvallisuuden varmistamista. Käytännössä kansallisen turvallisuuden¹ varmistamisen ja valtion turvallisuuden varmistamisen välinen ero on marginaalinen.

Keskusrikospoliisille tehtävää ilmoitusta ns. ylitörkeästä rikoksesta voitaisiin siirtää myös, jos se on välttämätöntä hengen ja terveyden suojaamiseksi. "Hengen ja terveyden suojaaminen" on välttämätöntä sisällyttää kansallisen turvallisuuden suojaamisen lisäksi toiseksi rikostiedon ilmoittamisen lykkäämisperusteeksi.

Momentin toisen virkkeen mukaan ilmoitusta saataisiin suojelupoliisin päällikön päätöksellä siirtää enintään vuodeksi kerrallaan ainoastaan, jos se on "välttämätöntä" kansallisen turvallisuuden varmistamiseksi tai hengen tai terveyden suojaamiseksi. Ilmoituksen siirtämiselle asetettaisiin siten korkea kynnys ("välttämätöntä"). Ilmoitusta voitaisiin siirtää enintään yhdeksi vuodeksi kerrallaan. Päätöksiä olisi kuitenkin mahdollista tehdä useampia, jos siihen olisi jokaisella kerralla esittää asianmukaiset perusteet.

Suojelupoliisin päällikön harkintavaltaa ohjaa myös² palomuurisäännöksen 3 momentti, jossa todetaan, että lykkäämispäätöksen arvioinnissa on otettava huomioon rikoksen selvittämisen tai sen estämisen merkitys yleisen ja yksityisen edun kannalta. Kyseistä säännöstä perustellaan seuraavasti (HE 202/2017 vp, s. 217):

Jotta suojelupoliisin päällikkö pystyisi tosiasiallisesti arvioimaan rikoksen selvittämisen tai rikoksen estämisen merkitystä yleisen ja yksityisen edun kannalta, niin tämä saattaisi yksittäistapauksellisesti edellyttää keskusrikospoliisille tai paikallispoliisille suoritettavaa tiedustelua ennen päätöksen tekemistä. Tällä turvattaisiin mainittujen intressien kohdalla se, että ne tulisivat suojelupoliisin päällikön päätösharkinnassa mahdollisimman täysimääräisesti turvattua.

Edellä kerrottu perustelulausuma huomioon ottaen Helsingin poliisilaitoksen lausunnossaan esittämä kritiikki on lähtökohtaisesti perusteetonta. Viitattakoon myös Poliisihallituksen lausunnossaan toteamaan, jonka mukaan 1 momentti ei muodostu poliisin kannalta käytännössä ongelmaksi, koska poliisi saanee monasti tiedon jo tapahtuneista vakavista rikoksista muutakin kautta kuin Suojelupoliisilta.

Suojelupoliisin on poliisilain 5 a luvun 61 §:n 2 momentin 3 kohdan perusteella mahdollisimman pian ilmoitettava tiedusteluvaltuutetulle päätöksestä, joka koskee 44 §:n 1 momentissa tarkoitettun ilmoituksen siirtämistä. Ilmoitus olisi myös merkittävässä osassa ulkoista valvontaa.

¹ Perustuslain muuttamista koskevassa esityksessä (HE 198/2017 vp, s. 35) kansallisella turvallisuudella viitataan viime kädessä valtion oikeudenkäyttöpiirissä olevien ihmisten kollektiiviseen turvallisuuteen välittömästi tai välillisesti väkivaltaista ulkoista uhkaa vastaan. Kansallisen turvallisuuden kannalta keskeisiä ovat sellaiset yhteiskunnan perustoiminnot, joiden häirintä tai lamauttaminen saattaisi viime kädessä johtaa ihmisten hengen tai terveyden vakavaan vaarantumiseen. Kansanvaltainen valtio- ja yhteiskuntajärjestys ja kansanvaltaisen yhteiskunnan instituutiot muodostavat perustan yhteisössä elävien ja toimivien ihmisten turvallisuudelle. Kansallisen turvallisuuden kannalta on merkityksellistä, että ylimmät valtioelimet ja muut julkisen vallan toimeilimet samoin kuin esimerkiksi yhteiskunnan perustoiminnoista huolehtivat voivat hoitaa tehtäviään ilman ulkoista häirintää. Kansallista turvallisuutta vakavasti uhkaavaa voi siten olla sellainenkin ulkoinen toiminta, joka tähtää kansanvaltaisen yhteiskunnan ja sen instituutioiden häirintään tai niiden toiminnan lamauttamiseen taikka mahdollistaa niiden toiminnan häirinnän tai lamauttamisen. (HE 198/2017 vp, s. 35–36)

² Suojelupoliisin päällikön harkintavaltaa ohjaavat aina poliisioikeudelliset periaatteet, kuten perus- ja ihmisoikeuksien kunnioittaminen, suhteellisuusperiaate, vähimmän haitan periaate ja tarkoitussidonnaisuusperiaate.

Poliisihallituksen mukaan 3 momentissa on harkinnanvaraisen tiedonluovuttamisen käyttöedellytyksiä tarkennettu Poliisinhallituksen aiemman esityksen suuntaisesti. Momentissa on kuitenkin lievä tekninen ongelma, eli sillä viitataan muun muassa koko 2 momenttiin, vaikka 2 momentissa on sekä pakottavia että harkinnanvaraisia osia. Pakottavien ilmoitusvelvollisuuksien osalta ei ole 2 momenttiin jätetty harkintavaltaa, eikä sitä tarvitsisi 3 momentilla siksi ohjata.

Sisäministeriön vastaus: Poliisihallituksen huomio on osin aiheellinen. Poliisilain 5 a luvun 44 pykälän 1-3 momentit kuuluvat seuraavasti:

Suojelupoliisin on ilman aiheetonta viivytystä ilmoitettava keskusrikospoliisille, jos tiedustelumenetelmän käytön aikana ilmenee, että voidaan olettaa tehdyksi sellainen rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta. Ilmoitusta saadaan suojelupoliisin päällikön päätöksellä siirtää enintään vuodeksi kerrallaan, jos se on välttämätöntä kansallisen turvallisuuden varmistamiseksi tai hengen tai terveyden suojaamiseksi. Suojelupoliisi saa ilmoittaa tehdystä rikoksesta keskusrikospoliisille, jos rikoksesta säädetty ankarin rangaistus on vähintään kolme vuotta vankeutta.

Suojelupoliisin on viipymättä ilmoitettava toimivaltaiselle viranomaiselle, jos tiedustelumenetelmän käytön aikana ilmenee, että hankkeilla on sellainen rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta, ja rikos on vielä estettävissä. Tiedustelumenetelmän käytöllä saatua tietoa saa luovuttaa toimivaltaiselle viranomaiselle sellaisen rikoksen estämiseksi, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta.

Kun harkitaan 1 momentissa tarkoitettua ilmoituksen siirtämistä tai 1 tai 2 momentissa tarkoitettua ilmoituksen tekemistä tehdystä rikoksesta, josta säädetty ankarin rangaistus on vähintään kolme vuotta vankeutta, tai sellaisen rikoksen estämisestä, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta, arvioinnissa on otettava huomioon rikoksen selvittämisen tai sen estämisen merkitys yleisen ja yksityisen edun kannalta.

Poliisihallitus viittaa pykälän 3 momenttiin, jossa viitataan myös 2 momentin 1. virkkeeseen, jota ei ole tarkoitettu säännöksessä harkinnanvaraiseksi. Pykälän 3 momentista voi saada vaikutelman, että myös 2 momentin 1. virkkeeseen sovellettaisiin 3 momentissa olevia punnintakriteerejä, koska siinä viitataan sellaisen rikoksen estämiseen, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta. Näin ei kuitenkaan pykälää ole tarkoitettu säädösteknisesti rakentaa, vaan 3 momentin punninta on ollut tarkoitus kohdistaa ainoastaan harkinnanvaraisiin luovutuksiin.

Kyseinen epäselvyys on mahdollista hoitaa tulkinnalla niin, että 3 momentissa olevia punnintakriteerejä sovelletaan 1 momentissa tarkoitettuun ilmoituksen siirtämiseen sekä 2 momentissa tarkoitettuihin ilmoituksen tekemisiin muilta osin kuin sellaisten estettävänä olevien ylitörkeiden rikosten osalta, joista tulisi ilmoittaa viipymättä.

Toisena vaihtoehtona on pykälän tekninen muutos niin, että 2 momentin 2. virke muutettaisiin uudeksi 3 momentiksi. Näin nykyisestä 3 momentista tulisi uusi 4 momentti, jossa olevat viittaukset kohdistettaisiin nykyiseen 1 ja uuteen 3 momenttiin.

Poliisihallituksen mukaan olisikin selvintä, että vielä estettävissä teoissa pakottava tiedonluovutus olisi kiinnitetty teon tai tapahtuman vaarapotentialiin, ei teon luonteeseen rikoksena tai rangaistuksen pituuteen. Kansallisen turvallisuuden todelliseksi takaamiseksi Suojelupoliisi tulisikin velvoittaa tiedonluovutukseen nykyehdotusta laajemmin tilanteissa, jossa teot voidaan estää. Siksi palomuurin nykyinen tulevaisuudessa ehkä tapahtuvan rikoksen ennakoituun rangaistushkaan kytkeytyvä ilmoittamisvelvollisuus ei ole paras mahdollinen.

Sisäministeriön vastaus: Poliisihallituksen tarkoittama uhkapotentiaali ilmenee pykälän 4 momentista, jonka mukaan tiedustelumenetelmän käytöllä saatua tietoa saa aina luovuttaa mukaan hengelle, terveydelle tai vapaudelle aiheutuvan merkittävän vaaran taikka huomattavan ympäristö-, omaisuus- tai varallisuusvahingon estämiseksi.

Helsingin poliisilaitos tiedustelee, että soveltuuko säännös myös siihen tilanteeseen, että esitutkintaviranomainen itse havaitsee rikosepäilyn, aloittaa esitutkinnan, minkä jälkeen se tiedustelee Suojelupoliisilta asiaan liittyvää mahdollista lisätietoa. Tiedustelun Suojelupoliisille tehdessään esitutkintaan jo suorittava poliisi kykenee yksilöimään rikosepäilyn keskeiset faktat kohtuullisen tarkasti teon, ajan, paikan, epäilyn / epäiltyjen ja mahdollisen asianomistajan osalta. Tällöin itse asia on jo tullut esitutkintaviranomaisen tietoon sen oman toiminnan tuloksena ennen kun tietopyyntö

tehdään Suojelupoliisille. Estettävissä olevan rikoksen osalta voidaan tehdä sama kysymyksenasettelu.

Sisäministeriön vastaus: Helsingin poliisilaitoksen mainitsemalle tiedustelulle ei ole estettä. Suojelupoliisi arvioi tapauskohtaisesti onko kyseessä sellainen tieto, joka siviilitiedustelua koskevan sääntelyn mukaan voidaan luovuttaa. Joissain tapauksissa, riippuen poliisin tiedustelun tietosisällön laadusta ja laajuudesta, tiedustelu voi auttaa suojelupoliisia suorittamaan tiedon luovuttamista koskevan intressipunninnan paremmin.

Helsingin poliisilaitos toteaa, että suojelupoliisi hankkii tietoja myös avoimista lähteistä, kansainvälisellä tietojenvaihdolla ja poliisilain 5 luvun mukaisilla keinoilla. Kyse voi olla myös sellaisesta tilanteesta, että kaikkia tai useita keinoja käytetään samassa asiassa. Koskeeko palomuurisäännös vain uusilla eli poliisilain 5 a luvun ja tietoliikennetiedustelusta siviilitiedustelusta annetun lain mukaisia keinoja käyttäen hankittuja tietoja vai kaikkia muitakin tiedustelukeinoilla hankittuja tietoja.

Sisäministeriön vastaus: Tältä osin viitataan otsikon "Viranomaisyhteistyö ja tietojen luovuttaminen" alla esitettyyn.

Helsingin poliisilaitos toteaa, että suojelupoliisin tiedonhankinnan kohteina voi olla samoja henkilöitä kuin poliisin rikostiedustelun tai tutkinnan kohteina. Voiko Suojelupoliisi luovuttaa tiedustelutoiminnassaan havaitsemia poliisin työturvallisuutta vaarantavia tietoja poliisille palomuurisäännöksen estämättä?

Sisäministeriön vastaus: Helsingin poliisilaitos viittaa lausunnossaan henkilötietojen käsittelystä poliisitoimessa annetun lain (761/2003) 2 §:n 3 momentin 6 kohtaan, jossa säädetään turvallisuustietojen tallettamisesta poliisiasian tietojärjestelmään. Suojelupoliisi olisi tiedustelulainsäädännön säätämisen jälkeen sisäministeriön alainen poliisiyksikkö. Näin ollen myös suojelupoliisi saa tallettaa poliisiasian tietojärjestelmään poliisilain 1 luvun 1 §:n 1 momentissa säädettyjen tehtävien suorittamiseksi hankittuja muita tarpeellisia tietoja seuraavasti: "--- 6) toimenpiteen kohteena olevan henkilön oman turvallisuuden tai viranomaisen työturvallisuuden turvaamiseksi välttämättömät tiedot henkilön terveydentilan ja sen seurannan taikka hänen sairautensa hoidon kannalta, tiedot kohteen tai henkilön vaarallisuudesta tai arvaamattomuudesta sekä tiedot, jotka kuvaavat tai on tarkoitettu kuvaamaan rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta (turvallisuustiedot); ---" Tätä asiointilaa ei ehdoteta muutettavaksi henkilötietojen käsittelystä poliisitoimessa annetun lain kokonaisuusdistuksen yhteydessä.

Helsingin poliisilaitos toteaa, että suojelupoliisin laajennetut tiedusteluvaltuudet tuovat sen tietoon todennäköisesti entistä enemmän sellaisia henkilöitä, jotka se on tähän asti siirtänyt paikallispoliisin vastuulle jatkokäsittelyyn. Suojelupoliisin resurssit eivät välttämättä riitä kaikkien vaaralliseksi luokiteltujen henkilöiden pidempiaikaiseen valvontaan ja heihin kohdistuvaan tiedonhankintaan eikä suojelupoliisin toimenkuvaan puhtaana tiedusteluviranomaisena sopine myöskään näkyvä kanssakäyminen kohdehenkilöiden kanssa. Sovelletaanko jatkossa näiden henkilöiden siirtoon palomuurisäännöstä, mikäli ne ovat tulleet Suojelupoliisin tietoon uusien tiedusteluvaltuuksien käytöllä tai muutoin?

Sisäministeriön vastaus: Henkilötietojen käsittelemiseen sovelletaan lakia henkilötietojen käsittelystä. Uhkahenkilöitä koskevien (henkilö)tietojen luovuttamiseen sovellettaisiin jatkossakin kyseistä lakia.

Helsingin poliisilaitos katsoo, että uhkan arviointitarve ei välttämättä liity vain yksittäisiin, tunnistettuihin uhkaa aiheuttaviin henkilöihin, vaan uhka-arviointia tehdään suojeltaviin kohteisiin liittyen. Helsingin poliisilaitos vastaa mm. Tasavallan presidentin ja valtioneuvoston jäsenten turvallisuudesta sekä turvaa valtiovierailut ja suurlähetystöjen koskemattomuuden. Vakiintuneesti poliisilaitos on tehnyt uhka-arvioinnin osalta yhteistyötä Suojelupoliisin kanssa ja yhtenä esimerkkinä tästä on mm. itsenäisyyspäivän juhlallisuuksien turvaaminen. Palomuurisäännös ei näyttäisi sallivan kovin hyvin tällaisen tiedon luovuttamisesta, ellei sitten tiedonsiirron katsota olevan mahdollista

ehdotetun poliisilain 5 a luvun 55 §:n nojalla, jonka mukaan Suojelupoliisi voi luovuttaa muille viranomaisille ja yhteisöille salassapitosäännösten estämättä tietoja, jos tietojen luovuttaminen on välttämätöntä kansallisen turvallisuuden suojaamiseksi.

Sisäministeriön vastaus: Poliisilain 5 a luvun 55 §:ssä ehdotetaan säädettäväksi yhteistyöstä muiden viranomaisten ja yhteisöjen kanssa. Pykälän 1 momentin mukaan suojelupoliisin on tarpeen mukaan toimittava yhteistyössä muiden viranomaisten kanssa siviilitiedustelun tarkoituksenmukaiseksi hoitamiseksi. Siviilitiedustelulla tarkoitetaan poliisilain 5 a luvussa tarkoitettua suojelupoliisin suorittamaa tiedonhankintaa ja tiedon hyödyntämisestä kansallisen turvallisuuden suojaamiseksi, ylimmän valtiojohdon päätöksenteon tukemiseksi ja muiden viranomaisten lakisääteisiä kansalliseen turvallisuuteen liittyviä tehtäviä varten. Usea Helsingin poliisilaitoksen esille nostama uhka kuuluu kansallisen turvallisuuden alaan, ja siten asiallisesti myös siviilitiedustelun piiriin.

Poliisilain 5 a luvun 55 §:n 2 momentin mukaan suojelupoliisi voi siviilitiedustelutehtävänsä toteuttamiseksi toimia yhteistyössä yhteisöjen kanssa sekä luovuttaa muille viranomaisille ja yhteisöille salassapitosäännösten estämättä tietoja, jos tietojen luovuttaminen on välttämätöntä kansallisen turvallisuuden suojaamiseksi. Tältä osin viitataan otsikon "Viranomaisyhteistyö ja tietojen luovuttaminen" alla lausuttuun. Sama koskee myös yleistä järjestystä ja turvallisuutta sekä informaatiovaikuttamista ja tilannekuvaa koskien.

VTT toteaa vertailumaiden lainsäädännöstä Norjan linjauksen kieltää tietoliikennetiedustelulla saatujen tiedon käytön oikeudessa kokonaan. Lisäksi VTT viittaa Ruotsin avoimuudesta onnistuneesta ennaltaehkäisystä voitaisiin ottaa mallia myös Suomessa

Sisäministeriön vastaus: Siviilitiedustelulainsäädäntöön ehdotetaan sisällytettäväksi ns. palomuuria koskeva säännös poliisilain muuttamista koskevan lakiehdotuksen 5 a luvun 44 §:ään. Siviilitiedustelulainsäädäntöä valmistelleessa työryhmässä pidettiin suomalaisen rikosoikeusjärjestelmän näkökulmasta kestävämmänä sellaista ratkaisua, jossa suomalaisella viranomaisella olisi tietoa törkeästä rikoksesta eikä sillä olisi velvollisuutta luovuttaa sitä toimivaltaiselle viranomaiselle tai että sellaisen tiedon luovuttaminen olisi kielletty kokonaan.

Ruotsin turvallisuuspoliisi kertoi tammikuussa 2015 estäneensä edeltävän puolentoista vuoden aikana kaksi terrori-iskua signaalitiedustelupalvelulta saamiensa tietoliikennetiedustelutietojen avulla. Asiasta tiedottaminen on poikkeuksellista, sillä tiedustelusta säätäneet maat eivät salassapitosyistä yleensä käsittele julkisuudessa sitä, millä nimenomaisella tiedustelumenetelmällä jotkin tiedot uhkatiedot on hankittu.

3 Siviilitiedustelun kohteet (Poliisilaki 5 a luku 3 § ja tietoliikennetiedustelulaki 3 §)

Ulkoministeriö katsoo lausunnossaan, että ehdotetun poliisilain uuden 5a luvun 3 §:ään sekä tietoliikennetiedustelusta siviilitiedustelusta annettavan lain 3 §:ään kirjatut uhkaluettelot ovat kattavia ja antavat omalta osaltaan kuvaa muuttuneesta ja haasteellisesta toimintaympäristöstä, jossa on tärkeää pyrkiä myös ennakoimaan mahdollinen vakava uhka kansalliselle turvallisuudelle. Ulkoministeriön arvion mukaan on tärkeää, että uhkaluettelot ovat samassa linjassa sotilastiedustelua koskevien lainsäädäntötekstien kanssa niiltä osin kuin tiedustelun kohteet koskevat molempia tiedustelulajeja. Kirjaukset hallituksen esityksissä näistä ovat hyvät.

Oikeusministeriö toteaa lausunnossaan, että tiedustelutoimivaltuuksien perusoikeuslottuvuukien vuoksi on erittäin tärkeää, että ehdotetut uudet tiedustelutoimivaltuudet kohdistuvat laissa tarkasti ja tyhjentävästi määritettyihin uhkiin sekä tiedustelumenetelmien käytön yleisiin ja erityisiin edellytyksiin.

Oikeuskansleri katsoo antamassaan lausunnossa, että turvallisuusviranomaisten toimivaltuuksia koskevan sääntelyn tulee lähtökohtaisesti olla täsmällistä ja tarkkarajaista. Toisaalta kansallista turvallisuutta vakavasti uhkaavaan toimintaan on toiminnallinen tarve puuttua aikaisessa vaiheessa. Uhkamäärittely jää tämän vuoksi väkisininkin joissain määrin väljäksi. Toimivaltuussääntelyn avoimuusasteeseen vaikuttaa sekä säännösten että niiden perustelujen osalta myös tarve pitää tiedusteluviranomaisten taktiset ja tekniset menetelmät salassa. On myös huomattava, että varhaisvaiheen tiedustelutoiminnassa ei ole perus-oikeusnäkökulmasta kyse tavanomaisesta konkreettinen perusoikeus vastaan toinen konkreettinen perusoikeus –punnintatilanteesta, vaan asetelmasta, jossa tiettyä konkreettista perusoikeutta (erityisesti yksityiselämän suoja) on arvioitava

suhteessa abstraktimpiin koko perusoikeus-järjestelmän olemassaolon edellytyksiin. Onhan kansallisessa turvallisuudessa viime kädessä kysymys kansakunnan elinmahdollisuuksien sekä kansanvaltaisuuteen ja oikeusvaltioperiaatteeseen perustuvan laillisen yhteiskuntajärjestyksen perusteiden turvaamisesta. Toimivaltuus-sääntelyn jonkinasteista väljyyttä voidaan kuitenkin kompensoida ja on kompensoitava toiminnan tehokkaalla valvonnalla ja hankittujen tietojen hyödyntämisrajoituksilla.

Eduskunnan oikeusasiamies toteaa, että hallituksen esityksessä ehdotetut tiedustelutoimivaltuudet ovat edelleen täsmällisyydeltään ja tarkkarajaisuudeltaan varsin etäällä nykyisten salaisten pakkokeinojen ja salaisten tiedonhankintakeinojen käyttöedellytyksistä ja käytön kohdentumisesta. Tämä johtuu keskeisesti tiedustelutoiminnan luonteesta

Korkein oikeus (KKO) katsoo, ettei siviilitiedustelun kohteita koskeva luettelo ei täysin täytä tämänkaltaiselle lainsäädännölle asetettavaa vaatimusta siitä, että tiedustelun edellytyksistä olisi säädettävä mahdollisimman täsmällisesti ja tarkkarajaisesti. Muun muassa kohdat 1 (terrorismi), 5 (kansanvaltaista yhteiskuntajärjestystä uhkaava toiminta) ja 7 (vieraan valtion toiminta, joka voi aiheuttaa vahinkoa Suomen kansainvälisille suhteille tai taloudellisille tai muille tärkeille eduille) ovat epäselviä ja voisivat mahdollistaa hyvinkin laajoja tulkintoja siviilitiedustelun sallituista kohteista. Käytettyjen käsitteiden tulkinnanvaraisuutta ja mahdollisten tulkintavaihtoehtojen laajuutta kuvaa esimerkiksi se, että perustelujen mukaan (s. 172) tiedustelun kohteena voisi olla myös terrorismi ilmiötasolla. Tosin tältä osin perusteluissa on esitetty konkretisointeja, jotka viittaavat siihen, ettei tiedustelun perusteeksi kuitenkaan tarkoiteta esittää aivan yleisen tason tietoa terrorismista. **KKO** kuitenkin toteaa, että käsitteiden laajuudesta ja tulkinnanvaraisuudesta aiheutuvaa ongelmaa olennaisesti vähentää se, että tiedustelumenetelmien käytön yleiset edellytykset [4 §:n 1 momentti] sisältävät merkittäviä kynnyksiä tiedustelun käytölle. Vaatimus tiedustelun kohteena olevan toiminnan aiheuttamasta vakavasta uhasta ja siitä, että tiedustelusta on perustellusti voitava olettaa saatavan tuloksia, antavat tuomioistuimelle edellytyksiä hoitaa sille kuuluvaa tehtävää tiedusteluvaltuuksien käytön kontrolloinnissa, kunhan huolehditaan siitä, että tuomioistuimilla on riittävästi tietoa.

Professori Olli Mäenpää toteaa, että vaikka ehdotettuun poliisilain 5 a luvun sääntelyyn sisältyy melko tulkinnanvaraisia käsitteitä, sitä voidaan tiedustelutoiminnan erityispiirteet huomioon ottaen pitää näiltä osin riittävänä toimivallan lakiperustaisuuden ja viranomaisen toiminnan lakisidonnaisuuden kannalta. Siviilitiedustelun toimivaltuudet voivat ehdotusten mukaan kuitenkin muotoutua käytännössä varsin laajoiksi, joten niiden sopeutumista perusoikeuksiin ja erityisesti luottamuksellisen viestinnän suojaan on arvioitava huolellisesti.

Amnesty toteaa, että listaus on kuitenkin niin laaja, epämääräinen ja tulkinnanvarainen, että jää käytännössä täysin tuomioistuinten päätöksenteon ja hakemuskäytännön varaan, millaisista uhkista tietoliikennetiedustelulla tullaan keräämään tietoa. Suojelupoliisin ja tuomioistuimen käytäntö tulevat ohjaamaan sitä, millaiset asiat voivat kuulua edellä mainittujen kohteiden piiriin.

Sisäministeriön vastaus: EIT on antanut 19. kesäkuuta 2018 ratkaisunsa tapauksessa Centrum för Rättvisa v. Ruotsi. Tuomiossaan EIT toteaa, että Ruotsin signaalitiedustelulaki asettaa kahdeksankohtaisen listan tilanteista, joissa signaalitiedustelua voidaan käyttää. Vaikka kohdat ovat osittain yleisluontoisia, niitä tarkennetaan lain esitöissä, jotka ovat olennainen lähde ruotsalaisessa lainsäädännössä. Tuomioistuin toteaa, että nämä kahdeksan tarkoitusta ("purposes") on asianmukaisesti indikoitu (tuomion kohta 120).³ EIT toteaa, että laissa säädetään riittävän selkeällä tavalla toimivaltuuksien käytön perusteista sekä niiden käyttämisestä (tuomion kohta 124).

³ Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet

1 §

I försvarsunderrättelseverksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet får den myndighet som regeringen bestämmer (signalspaningsmyndigheten) inhämta signaler i elektronisk form vid signalspaning. Signalspaning i försvarsunderrättelseverksamhet får endast ske i de fall regeringen eller en myndighet som anges i 4 § närmare har bestämt inriktningen av signalspaningen.

Signalspaning i försvarsunderrättelseverksamhet får ske endast i syfte att kartlägga

1. yttre militära hot mot landet,
2. förutsättningar för svenskt deltagande i fredsfrämjande och humanitära internationella insatser eller hot mot säkerheten för svenska intressen vid genomförandet av sådana insatser,
3. strategiska förhållanden avseende internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen,

Toiminnan vakavuutta koskeva edellytys ilmenee tiedustelumenetelmien käytön edellytyksiä koskevasta 4 §:stä. Pykälän 1 momentissa ehdotetaan säädettäväksi kaikille tiedustelumenetelmille yhteisestä yleisestä käyttöedellytyksestä ”voidaan perustellusti olettaa saatavan tietoja sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta”. Kyse on perustelua edellyttävästä tuloksellisuusvaatimuksesta, jolloin tiedustelumenetelmän käytön odotusarvona on sen perusteltu hyödyllisyys. Siviilitiedustelun kohteena olevalla toiminnalla tarkoitetaan 3 §:ssä (Siviilitiedustelun kohteet) tarkoitettua toimintaa. Perusteluedellytys liittyy myös siihen, että 3 §:ssä tarkoitettua toimintaa vastaan olisi perusteltua syytä ryhtyä suojautumaan. Kansallista turvallisuutta vakavasti uhkaavan toiminnan vaatimus johtuu ehdotettavan perustuslain 10 §:n 4 momentista (HE 198/2017 vp.). Kyseisen perustuslain kohdan perusteella vakavuusedellytys nostaa luottamuksellisen viestin suojaan puuttuvien keinojen soveltamiskynnystä asettaessaan kvalifioinnin uhkan laadusta. Siten pelkästään jonkinasteisen uhkan kansalliselle turvallisuudelle muodostava toiminta ei vielä täyttäisi säännöksessä asetettua vaatimusta. Uhkan vakavuusaste kytkeytyy myös edellä 3 §:ssä käsiteltyihin sisällöllisiin määrittelyihin siitä, millainen siviilitiedustelun kohteena oleva toiminta muodostaa vakavan uhkan kansalliselle turvallisuudelle.

On huomattava, että kansallista turvallisuutta vakavasti uhkaava toiminta saa uusia muotoja ajan kuluessa ja tekniikan kehittyessä. Kansalliseen turvallisuuteen kohdistuvat uhkat kohdistuvat yhteiskuntaan kokonaisuutena. Uhkat ovat luonteeltaan sellaisia, että niiden toteutuessa koko yhteiskunnalle aiheutuu merkittävää vahinkoa niin taloudellisesti, yhteiskuntajärjestyksen kuin elintavan osalta. Uhkat voivat myös konkretisoida ennakoimattomasti ja täysin uuden tyyppisten uhkien määrittely etukäteen on mahdotonta (EIT Centrum för Rättvisa v. Ruotsi kohta 119). Tästä syystä tiedustelutoiminnan tulee olla tehokasta ja aina eteenpäin katsovaa. Hankitun tiedon pohjalta ylin valtiojohto voi ryhtyä proaktiivisesti tarpeellisiin toimenpiteisiin alati muuttuvassa turvallisuusympäristössä.

Sisäministeriö katsoo, että siviilitiedustelun kohteita koskevat poliisilain 5 a luvun 3 §:n ja tietoliikennetiedustelulain 3 §:ien kohdeluettelot ovat EIT:n ratkaisussa Centrum för Rättvisa v. Ruotsi (kohta 120) mukaisen sekä myös aiemman EIT:n tulkintakäytännön vaatimukset täyttyviä ja esitettyjen säännösten voidaan katsoa olevan riittävän selkeitä sekä täsmällisiä ja tarkkarajaisia.

VTT kritisoi kaksikäyttötuotteiden kuulumista siviilitiedustelun kohteisiin, koska viime aikoina myös erilaiset tieto- ja kyberturvallisuusohjelmistot ja -työkalut on haluttu nähdä kaksikäyttötuotteina. Joissakin maissa tulkinnot tai niiden epäselvyys ovat johtaneet tilanteisiin, joissa jopa salausmenetelmiin liittyvien teknisten ja matemaattisten menetelmien opettaminen vaihto-opiskelijoille voitaisiin nähdä kaksikäyttötuotteen luvattomana levittämisenä.

Sisäministeriön vastaus: Siviilitiedustelun kohteista ehdotetaan säädettäväksi poliisilain 5 a luvun 3 §:ssä. Ainoastaan siviilitiedustelun kohteista voitaisiin hankkia tietoa tiedustelumenetelmiä käyttäen. Siviilitiedustelun kohdeluettelo olisi tyhjentävä. Tietoliikennetiedustelusta siviilitiedustelussa ehdotettavan lain 3 §:ään ehdotetaan otettavaksi samansisältöinen säännös kansallista turvallisuutta vakavasti uhkaavasta toiminnasta.

Mainitun pykälän 4 kohdan mukaan tiedustelumenetelmiä saisi käyttää tiedon hankkimiseksi kaksikäyttötuotteiden vientivalvonnasta annetun lain (562/1996) 2 §:ssä tarkoitettujen kaksikäyttötuotteiden suunnittelusta, valmistamisesta, levittämisestä ja käytöstä.

Kaksikäyttötuotteilla tarkoitetaan kaksikäyttötuotteiden vientivalvonnasta annetun lain 2 §:n mukaan tuotetta, teknologiaa, palvelua ja muuta hyödykettä, jota normaalin siviililuontoisen käyttönsä tai sovellutuksensa ohella voidaan käyttää joukkotuhousohjeiden tai niiden maaliin saattamiseen tarkoitettujen ohjusjärjestelmien kehittelyyn tai valmistukseen taikka jolla voidaan edistää yleistä sotilaallista toimintakykyä. Kaksikäyttötuotteiden vientivalvonnan tärkeimpänä tavoitteena on joukkotuhousohjeiden leviämisen estämiseen tähtäävä asesulkupolitiikka.

-
4. utveckling och spridning av massförstörelsevapen, krigsmateriel och produkter som avses i lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd,
 5. allvarliga yttre hot mot samhällets infrastruktur,
 6. konflikter utomlands med konsekvenser för internationell säkerhet,
 7. främmande underrättelseverksamhet mot svenska intressen, eller
 8. främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- eller försvarspolitik.

Kaksikäyttötuotteiden suunnittelu, valmistaminen, levittäminen ja käyttö voisi ilmetä esimerkiksi kaksikäyttötuotteiden hankkimisena, kauttakuljetuksena tai välityksenä vastoin voimassa olevaa vientivalvontalainsäädäntöä taikka Euroopan unionin rajoittavia toimenpiteitä tai Yhdistyneiden kansakuntien asettamia pakotteita. Tietoa voitaisiin hankkia esimerkiksi ulkomaisen toimijan pyrkimyksistä, suunnitelmista tai valmisteluista hankkia vilpillisesti tai harhauttamalla suomalaiselta yritykseltä kaksikäyttötuotteita EU:n tai YK:n asettamien pakotteiden vastaisesti.

Huomioitavaa tiedustelumenetelmän käytössä on kuitenkin menetelmän käytön edellytykset, joista ehdotetaan säädettäväksi poliisilain 5 a luvun 4 §:ssä. Jokaisen tiedustelumenetelmän käytön yleisenä edellytyksenä siviilitiedustelussa on, että sillä voidaan perustellusti olettaa saatavan tietoja sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta (1 momentti). Sen lisäksi, mitä tiedustelumenetelmien käytön erityisistä edellytyksistä jäljempänä säädetään, telekuuntelua, tietojen hankkimista telekuuntelun sijasta, suunnitelmallista tarkkailua, teknistä kuuntelua, teknistä katselua, henkilön teknistä seuranta, teknistä laitetarkkailua, peitetoimintaa, valeostoa, tietolähteen ohjattua käyttöä ja paikkatiedustelua saadaan siviilitiedustelussa käyttää vain, jos niillä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi 1 momentissa tarkoitettusta toiminnasta. Peitetoiminnan ja valeoston käyttäminen edellyttää lisäksi, että menetelmän käyttö on välttämätöntä. Peitetoiminnan käyttäminen edellyttää myös, että tiedonhankintaa on toiminnan suunnitelmallisuuden, järjestäytyneisyyden tai ammattimaisuuden taikka ennakoitavissa olevan jatkuvuuden tai toistuvuuden vuoksi pidettävä tarpeellisena (2 momentti).

Kuten muidenkin siviilitiedustelun kohteiden kohdalla, niin myös kaksikäyttötuotteiden suunnittelun, valmistamisen, levittämisen ja käytön tulee toimintana olla perustellusti ja oletettavasti sellaista, että kyseinen toiminta vakavasti uhkaa Suomen kansallista turvallisuutta.

4 Salaisen tiedonhankinnan yhteensovittaminen (Poliisilaki 5 a luku 56 §)

POHA katsoo, että hallituksen esityksessä ehdotettu koordinaatiota koskeva pykäläluonnos on sisällöllisesti käytännössä riittämätön ehdollisella muotoilullaan ("...on tarvittaessa yhteen sovitettava..."). Toki jo tällä hetkellä voidaan toimia yhteen sovittaa ilman, että siitä laissa erikseen säädetään. Lain ration varmistamiseksi tulisi pykälässä olla pakottava muotoilu, jotta koordinaatiolla olisi käytännössä merkitystä. Tämä voidaan toteuttaa poistamalla sana tarvittaessa. Nykymuodossa koordinointi jää vapaaehtoisuuden varaan ja jättää vaaran päällekkäisille operaatioille. Mikäli ehdotettu muotoilu jää voimaan, niin vähintäänkin Valtioneuvoston asetus tulisi antaa mahdollisimman pikaisesti, jotta asia saataisiin täsmennettyä.

Keskusrikospoliisi toteaa, että ehdotetussa siviilitiedustelua koskevassa laissa Keskusrikospoliisi asema korostuu muun muassa yhteistyöviranomaisena. Käytännössä esimerkiksi terrorismi-valtiopetosrikokset tulevat Keskusrikospoliisin tutkittaviksi. Näin ollen Keskusrikospoliisi pitää tärkeänä, että ehdotetussa säännöksessä säädettäisiin siitä, että asetuksella voitaisiin säätää tarkemmin Keskusrikospoliisin ja Suojelupoliisin yhteistyön järjestämisestä.

Sisäministeriön vastaus: Sisäministeriö ei katso tarpeelliseksi muuttaa lakiehdotuksen kohtaa velvoittavaan muotoon. Pykäläluonnoksen muotoilun ("...on tarvittaessa yhteen sovitettava...") tarkoitus on olla mahdollistava, ei velvoittava. Jos viranomaiset, joilla mm. on oikeus käyttää salaista tiedonhankintaa katsovat, että yhteensovittamisen tarve on olemassa, niin pykälä mahdollistaisi niiden välisen koordinaation. Nykyisellään esimerkiksi valtakunnan vakavan rikollisuuden kohdetorjuntamenettely, johon osallistuvat Poliisi, Rajavartiolaitos ja Tulli, on hyvä esimerkki viranomaisten välisestä koordinaatiosta.

Poliisilakiehdotuksen 5 a luvun 62 §:ssä ehdotetaan säädettäväksi asetuksenantovaltuuksista. Pykälän 1 momentin 7 kohdan mukaan valtioneuvoston asetuksella voitaisiin säätää tiedonhankinnan yhteensovittamisen järjestämisestä. Asetuksella voitaisiin tarvittaessa säätää tarkemmin mm. menettelyistä miten salaista tiedonhankintaa voitaisiin yhteen sovittaa.

Eri hallinnonalojen salaista tiedonhankintaa toteuttavat keskeiset toimijat ovat nykyisin edustettuina salaisen tiedonhankinnan seurantaryhmässä. Esitutkinnasta, pakkokeinoista ja salaisesta tiedonhankinnasta annetun valtioneuvoston asetuksen (122/2014) 3 luvun 21 §:ssä säädetään salaisen tiedonhankinnan seurannasta. Ryhmän tehtävänä on mm. toiminnan, yhteistyön ja koulutuksen seuranta sekä kehittämis ehdotusten tekeminen. Esimerkiksi vuonna 2017 seurantaryhmä kokoontui neljä kertaa käsitellen seuraavia aiheita:

- televalvonnan edellytyksistä ja rajanvedosta kuolemansyöntutkintaan,
- koulutustarpeista netissä tapahtuvaan valeosto- ja peitet toimintaan,
- netin pikaviestipalvelut,
- salaisten tiedonhankintakeinojen ohjeistuksen päivittäminen,
- valmisteilla olevan tiedustelulain vaikutuksista ja rajapinnoista ns. perinteiseen salaiseen tiedonhankintaan sekä muita ajankohtaisia asioita.⁴

Seurantaryhmällä on melko itsenäinen valta päättää seurantakohteet ja ryhmässä käsiteltävät asiat. Seurantaryhmällä on näin ollen mahdollista ottaa käsiteltäväkseen myös salaisen tiedonhankinnan yhteensovittamista koskevia asioita.

5 Suojelupoliisin poliisius

POHAN katsoo lausunnossaan, että lakipakettia rasittaa ongelma siitä, että suojelupoliisi jää osaksi poliisia ja heidän poliisimiehillä olisi yhä poliisivaltuudet. Nämä valtuudet tuovat mukanaan myös velvollisuuksia. Poha katsoo olevan juridisesti hankalaa olla samaan aikaan tiedusteluviranomainen ja poliisi.

Sisäministeriön vastaus: Poliisilain 5 a luvun 36 §:ssä ehdotetaan säädettäväksi tiedonhankinnan suojaamisesta vastaavalla tavalla kuin 5 luvun 46 §:n 2 ja 3 momentissa. Kyseisen 46 §:n 1 momentissa tarkoitettu puuttumisen siirtämisestä ei olisi tarpeen säätää 5 a luvussa, koska suojelupoliisin poliisimiehen puuttumis- tai toimimisvelvollisuus tulisi katettua poliisin hallinnosta annetun lain 15 c §:n 3 momentissa ja tämän luvun 44 §:ssä olevalla sääntelyllä (HE 202/2017 vp., s. 208).

Poliisin hallinnosta annetun lain 15 c §:n 3 momentissa on kyse niin sanotusta jokaiselle poliisimiehelle kuuluvasta toimimisvelvollisuudesta. Poliisimiehen toimimisvelvollisuuden syntymiselle on myös asetettu eräitä edellytyksiä, kuten kiireellisyys ja välttämättömyys. Vakavan rikoksen estäminen ja tutkinnan aloittaminen saattaa tarkoittaa pelkästään ilmoituksen tekemistä alueella toimivalle poliisiyksikölle. Velvollisuus sisältää ainakin ne vähimmäistoimenpiteet, jotka on välttämättä suoritettava säännöksessä tarkoitetun tuloksen saavuttamiseksi. Poliisimiehen toimimisvelvollisuus on siis mahdollista täyttää esimerkiksi tekemällä hälytyskeskukselle ilmoitus antaen asiaa koskevat tarvittavat tiedot. Tässä yhteydessä ei ole tarpeen ilmoittaa sellaisia tietoja, jotka saattaisivat johtaa siviilitiedustelun paljastumiseen tai aiheuttaa työturvallisuusriskin. Esimerkiksi jos tilanne edellyttäisi, niin ilmoituksen voisi tehdä käyttäen peitehenkilöllisyyttä tai ilmoituksen voisi tehdä myös anonyymisti.

Poliisin hallinnosta annetun lain 15 c §:n 3 momentissa tarkoitettu vakavan rikoksen käsite on riippuvainen ensinnäkin tilanteesta kokonaisuudessaan ja myös rikoksen kohteena olevasta henkilöstä ja tämän mahdollisuuksista puolustautumiseen. Jos rikos on kohdistumassa pieneen lapseen tai sairauteen, iän tai muun syyn vuoksi puolustuskyvyttömään henkilöön, kenen mahdollisuudet puolustautua ovat vähäiset, niin tämä edellyttäisi intensiivisempää toimimisvelvollisuutta siviilitiedustelua hoitavalta poliisimiehellä kuin jos kyse olisi rikoksen kohdistumisesta puolustuskykyiseen aikuiseen henkilöön. Kyse on aina tapauskohtaisesta harkinnasta.

Poliisilain 5 a luvun 44 §:ssä (Tiedon luovuttaminen rikostorjuntaan) ehdotettava säännös olisi erityissäännös suhteessa poliisin hallinnosta annetun lain 15 c §:n 3 momenttiin nähden, koska se muodostaa toimimisvelvollisuuden osalta kvalifioitun velvollisuuden puuttua sellaisiin rikoksiin, joista säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta (44 §:n 1 ja 2 momentti). Tämä liittyy poikkeuksesta tilanteeseen, jolloin suojelupoliisin poliisimies on virantoimituksessa, koska 44 §:ssä tarkoitetaan tilanteita, jolloin tiedustelumenetelmän käytön aikana ilmenee sellaista tietoa, jonka perusteella olisi mahdollista estää vakava rikos tai luovuttaa merkityksellistä tietoa rikoksen selvittämiseksi. Poliisin hallinnosta annetun lain 15 c §:n 3 momentissa tarkoitettujen tilanteiden ulottuvat myös virantoimituksen ulkopuolelle poliisimiehen vapaa-ajalle.

Poliisin hallinnosta annetun lain 15 c §:n 3 momentissa säädetty poliisimiehen toimimisvelvollisuus ja 44 §:ää koskeva sääntely eivät muodosta ristiriitaa, vaikka säännöksissä ilmenee kuitenkin vakavan rikoksen estämisen kohdalla päällekkäisyyttä. Tiedon luovuttamisessa rikostorjuntaan olisi kyse

⁴ Salaista tiedonhankintaa koskeva kertomus vuodelta 2017 (SMDno-2018-337), s. 38.

tarvittavien tietojen luovuttamisesta rikoksen estämiseksi tai selvittämiseksi, jotta toimivaltainen viranomais voisi ryhtyä tarvittaviin toimiin. Ilmoitusvelvollisuus tai -oikeus perustuisi kuitenkin tiedustelumenetelmän käytön aikana saatuihin tietoihin, kun taas poliisimiehen toimimisvelvollisuus on riippumaton ajasta, paikasta ja siitä onko poliisimies virantoimituksessa vai ei. Tiedustelumenetelmien käytön aikana ilmenevän rikoksen kohdalla poliisimiehen toimimisvelvollisuus tulisi lähtökohtaisesti täytettyä 44 §:n mukaan tehtävällä ilmoituksella. Jos siviilitiedustelua toteuttava poliisimies voisi operaatioturvallisuuden sekä työturvallisuuden mahdollistaessa puuttua henkilökohtaisesti vakavan rikoksen estämiseen, 44 §:n sääntely ei tätä estäisi.

6 Toimivaltuudet (Tiedustelumenetelmät)

6.1 Tietoliikennetiedustelun käytön edellytykset

Eduskunnan oikeusasiamies toteaa lausunnossaan, että muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuva tiedustelu olisi 4 §:n 2 momentin mukaan mahdollista, jos tiedustelun "voidaan olettaa olevan välttämätöntä" tiedon saamiseksi tiedustelutehtävän kannalta".

Kysymyksen alaista on, täyttääkö tämä kynnys perusteluissa selostetun Szabo & Vissy v. Unkari – tuomion vaatimuksen yleisestä ja yksittäistapauksellisesta ehdottomasta välttämättömyydestä ("strictly necessary").

Sisäministeriön vastaus: Välttämätön demokraattisessa yhteiskunnassa -edellytys pitää sisällään sen, että oikeuksiin puuttumisen tulee vastata pakottavaan yhteiskunnalliseen tarpeeseen (correspond to a pressing social need). Edellytyksestä seuraa myös, että puuttumisen on oltava suhteellisuusperiaatteen mukaista: puuttumisen on oltava järkevässä suhteessa siihen EIS 8(2) artiklan sallimaan tavoitteeseen, johon vedotaan oikeuttamisperusteena (mm. Gillow v. Yhdistynyt Kuningaskunta, Silver ja muut v. Yhdistynyt Kuningaskunta, Handyside v. Yhdistynyt Kuningaskunta).

Puuttumisen välttämättömyyden arviointi niin yhteiskunnallisen tarpeen pakottavuuden kuin suhteellisuudenkin näkökulmasta kuuluu ensisijaisesti tai ainakin ensi vaiheessa kansalliselle lainsäätäjälle ja kansallisille viranomaisille (Silver ja muut v. Yhdistynyt Kuningaskunta, Handyside v. Yhdistynyt Kuningaskunta). Tätä arviointia suorittaessaan kansallisilla tahoilla on tiettyä harkintamarginaalia, jonka laajuutta määrittää muun muassa se, mitä EIS:n takaamaa oikeutta puuttuminen koskee, se, kuinka syvällekyvästä puuttumisesta on kyse, sekä se, mikä EIS 8(2) artiklan sallima tavoite on puuttumisen oikeuttamisperusteena. Harkintamarginaali on tavanomaista väljempi silloin, kun oikeuttamisperusteena on kansallinen turvallisuus (Klass ja muut v. Saksa, Leander v. Ruotsi). Kansallisen turvallisuuden kysymyksissä valtion melko laaja harkintavalta koskee myös niitä konkreettisia keinoja ja menetelmiä, joiden avulla se kyseistä etua suojaa. Ratkaisussaan Weber ja Saravia v. Saksa EIT katsoi, että valtio sille kuuluvan harkintavallan puitteissa oli voinut säätää laajamittaisesta viestintäyhteyksien valvonnasta menetelmänä suojata kansallista turvallisuuttaan. Kyse oli demokraattisessa yhteiskunnassa välttämättömästä puuttumisesta EIS 8 artiklan yksityisille oikeussubjekteille takaamiin oikeuksiin.

Tietoliikennetiedustelua Weber & Saravia -ratkaisun tavoin koskevissa Zakharov- ja Szabo & Vissy -ratkaisuissaan EIT kuitenkin täsmensi välttämättömyyskriteeriä tavalla, joka näyttäisi eräiltä osin kaventavan yllä mainittua valtion harkintavaltaa. Silloin kun kyse on tietoliikennetiedustelun kaltaisen kehityksen kärkeä edustavan valvontateknologian käytöstä, on "välttämätön demokraattisessa yhteiskunnassa" -edellytystä tuomioistuimen mukaan tulkittava siten, että se edellyttää "ehdotonta välttämättömyyttä" (strict necessity) kahdessakin suhteessa. Ensinnäkin salaisen tarkkailutoimenpiteen tulee olla yleisellä tasolla ehdottoman välttämätön demokraattisten instituutioiden suojaamiseksi. Toiseksi toimenpiteen tulee olla yksittäisen tiedusteluoperaation yhteydessä ehdottoman välttämätön olennaisen tärkeän tiedon (vital information) saamiseksi.

Tietoliikennetiedustelun yleisistä edellytyksistä säädettäisiin lain 4 §:ssä. Kaiken tietoliikennetiedustelun edellytyksenä olisi perusteltu toiminnan tuloksellisuus. Pelkkä perusteltu tuloksellisuusodotus soveltuisi silloin, kun tietoliikennetiedustelu voidaan kohdistaa pelkästään valtiollisen toimijan tai siihen rinnastuvan tahon tietoliikenteeseen. Valtiolliseen toimijaan rinnastuvalla taholla tarkoitettaisiin valtionomaisen rakenteen omaavaa toimijaa, joka määrättyllä alueella käyttää omintakeista ja pysyvää valtaa. Pelkän perustellun tuloksellisuusodotuksen soveltaminen perustuisi siihen, että valtiot ja niihin rinnastuvat tahot eivät nauti viestintäsalaisuutta.

Muissa tapauksissa tietoliikennetiedustelun yleisenä edellytyksenä olisi tuloksellisuuden lisäksi välttämättömyys, mikä on korkein poliisin toimivaltuuksia koskevan lainsäädännön tuntema

edellytyskynnys. Välttämättömyysedellytystä sovellettaisiin sekä niissä tapauksissa, joissa tietoliikennetiedustelun kohteena sinänsä on vieras valtio, mutta hakehtojen käytön piiriin voi tulla muutakin tietoliikennettä, että niissä tapauksissa, joissa tietoliikennetiedustelun kohde nauttii luottamuksellisen viestin salaisuutta.

Tietoliikennetiedustelulle asetettaisiin tiukempi edellytys kuin poliisilain 5 a luvussa säädettäväksi ehdotetuille viestintään kohdistuville tiedustelumenetelmille. Ratkaisun taustalla on Euroopan ihmisoikeustuomioistuimen ratkaisu Szabo & Vissy v. Unkari, jonka mukaan tietoliikennetiedustelun käytön tulisi olla yleisellä tasolla ehdottoman välttämätöntä demokraattisten instituutioiden suojaamiseksi, ja yksittäisen tiedusteluoperaation yhteydessä ehdottoman välttämätöntä olennaisen tärkeän tiedon saamiseksi. Lain 3 §:ssä yksilöidyt tietoliikennetiedustelun kohteet kohdistuvat demokratiaan ja sen keskeisiin instituutioihin, jolloin tietoliikennetiedustelussa voidaan katsoa olevan kyse demokratian suojelemiseksi välttämättömästä toimivaltuuden käytöstä. Säättämällä tietoliikennetiedustelun edellytykseksi välttämättömyys vastattaisiin vaatimukseen, että tietoliikennetiedustelun käytön tulee olla yksittäistapauksessa ehdottoman välttämätöntä. Ihmisoikeustuomioistuimen "ehdottoman välttämättömyyden" ja kansallisen toimivaltuuslainsäädännön korkeimpana kynnyksenä olevan "välttämättömyyden" välillä on vaikea nähdä mitään ratkaisevaa eroa. Myös Ruotsin ja Sveitsin lainsäädännöissä edellytyskynnykseksi on asetettu välttämättömyys.

Tietoliikennetiedustelun välttämättömyydellä tarkoitettaisiin viimesijaisuutta eli sitä, että tietojen hankkiminen muulla keinolla olisi mahdotonta tai kohtuuttoman vaikeaa. Edellytyksen soveltaminen edellyttäisi sekä tietoliikennetiedusteluun lupaa hakevalta suojelupoliisilta että lupavaatimuksen ratkaisijana olevalta tuomioistuimelta vertailua yhtäältä poliisilain 5 a luvussa tarkoitettujen menetelmien sekä toisaalta tietoliikennetiedustelun välillä. Jos muiden tiedustelumenetelmien käyttö ei olisi mahdotonta tai kohtuuttoman vaikeaa, tulisi niitä käyttää ensisijaisina keinoina suhteessa tietoliikennetiedusteluun. Lain 4 §:n 3 momentissa olisi välttämättömyysvaatimusta täsmentävä ja sitä suhteessa teletiedonhankintakeinoin entisestään tiukentava säännös, jonka mukaan tietoliikennetiedustelun hakehtona ei saataisi lainkaan käyttää Suomessa olevan telepäätelaitteen tai teleosoitteen yksilöintitietoa. Jos suojelupoliisilla olisi hallussaan tällainen tieto, se ei saisi ylipäättään käyttää tietoliikennetiedustelua, vaan sen tulisi käyttää telekuuntelua, televalvontaa tai muita poliisilain ehdotetussa 5 a luvussa säädettyjä teletiedonhankintatoimivaltuuksia.

Szabo & Vissy –tapausta, kuten muitakin EIT:n ratkaisuja, on tarpeen arvioida myös arvioitavaa lainsäädäntökehikkoa vasten. Szabo & Vissy –ratkaisun mukaan *Unkarin* lainsäädäntö antoi viranomaisille mahdollisuuden kohdentamattomaan tiedusteluun eikä lainsäädäntö ollut kohdentamisen osalta riittävän selkeä sen osalta, ketkä tiedustelun kohteeksi saattoivat joutua.

Ensinnäkin EIT toteaa ratkaisussaan (kohta 64), että Unkarin lainsäädäntö ei ole riittävän tarkkarajainen, jotta sen perusteella voitaisiin arvioida tiedustelutoimivaltuuksien kohdentumista. Unkarin lainsäädännön perusteella lähes kuka vain voi joutua tiedustelun kohteeksi (kohta 66, 67 ja 70).

Toiseksi päätöksen tiedustelutoimivaltuuden käyttämisestä tekee poliittinen päätöksentekijä, oikeusministeri, joka ei arvioi tiedusteluviranomaisen hakemusta oikeudellisesti (kohdat 57, 71, 73, 75 ja 76).

Kolmanneksi tiedusteluviranomaisen ei tarvinnut riittävällä tarkkuudella perustella ja esittää tosiseikastoa hakemuksensa tueksi, mistä kävisi ilmi tiedustelutoimivaltuuden käytön tarkoitus ja kohdistuminen (kohta 71, 79 ja 81).

Neljänneksi tiedustelutoiminnan ulkopuolinen, riippumaton ja oikeudellinen valvonta oli puutteellista ja kyseenalaista, sillä valvonnasta vastuussa oli sisäministeri (kohta 78). Lisäksi parlamentaarinen valvonta todettiin puutteelliseksi eikä vuosittaiset raportit olleet julkisia (kohta 82).

Viidenneksi tiedustelutoimivaltuuden käytön kohteelle ei annettu ilmoitusta, jotta kohde olisi voinut ryhtyä tarvittaviin toimiin eikä kohteella ollut muutenkaan oikeusturvakeinoja käytössään (kohta 86), tiedustelutoimivaltuuden käytön kohteella ei ole mitään riittäviä keinoja oikeus-suojansa toteuttamiseksi (kohta 86) eikä tiedustelutoimivaltuuden käytön kohde voi saattaa asiaa ulkopuolisen puolueettoman tahon käsiteltäväksi (kohta 83).

Kuudenneksi Unkarin lainsäädäntö ei velvoittanut tiedusteluviranomaista tuhoamaan hankkimaansa ylimääräistä tietoa, vaan mahdollisti sen laajan käytön.

EIT on antanut 19. kesäkuuta 2018 ratkaisun tapauksessa Centrum för Rättvisa v. Ruotsi. Tapauksessa voittoa tuottamaton yhteisön valitus koski sitä, että Ruotsin valtion signaalitiedustelua

koskevat käytännöt ja lainsäädäntö rikkoivat ja rikkovat Euroopan ihmisoikeussopimuksen (EIS) takaamaa oikeutta nauttia yksityis- ja perhe-elämän suojaa.

EIT toteaa ratkaisussaan Centrum för Rättvisa v. Ruotsi, että signaalitiedustelun osalta arvio siitä, rikkooko valtion lainsäädäntö EIS:n 8 artiklaa, on tehtävä kokonaisharkintana (kohta 180). Ratkaisussaan EIT ei mainitse sitä, että Ruotsin lainsäädännössä signaalitiedustelun käytön edellytyksenä olisi "ehdoton välttämättömyys" tai "täysin välttämätöntä".

Tapauksessa Centrum för Rättvisa v. Ruotsi EIT toteaa, että signaalitiedustelu aiheuttaa uhan yksityisyyden suojalle, mutta toisaalta ymmärtää käsiteltävänä olevassa tapauksessa olevan kansallisen turvallisuuden suojaamisen järjestelmän merkittävyyden. EIT toteaa myös, että Ruotsin järjestelmä täyttää niin kutsutun Venetsian komitean suositukset (kohta 179), kuten lupapäätösprosessille asetetut suositukset ja riippumaton ulkopuolinen valvonta.

EIT toteaa ratkaisussaan, että vaikka Ruotsin lainsäädännön soveltamisala on laaja (kohta 112), kuitenkin viranomaisten toimintaa on viestintään puuttumisen osalta rajoitettu (kohta 180). EIT:n mukaan Ruotsin lainsäädäntö minimoi yksityisyyden suojan loukkauksia ja kompensoi avoimuuden puuttumisen. Signaalitiedustelun soveltamisala ja tiedustelun kohteeksi päätyneet tietoliikenteen käsittely on selkeästi määritelty laissa, päätöksentekomenettely on yksityiskohtainen ja annettu oikeudelliselle päätöksentekijälle sekä useat ulkopuoliset tahot (ulkopuolinen valvontaelin, oikeuskansleri, oikeusasiamies ja tietosuojavaltuutettu) valvovat ja arvioivat toimintaa (kohta 180).

EIT:n ratkaisussa todetaan vielä nimenomaisesti, että Ruotsin lainsäädäntö antaa riittävän suojan signaalitiedustelun käyttämisestä mielivaltaisesti ja muita väärinkäytöksiä vastaan (kohta 181).

Ruotsin lainsäädännön katsotaan täyttävän lainsäädännöltä edellytettävät laatuvaatimukset ja yksityis- ja perhe-elämän suojaan puuttumisen olevan välttämätöntä demokraattisessa yhteiskunnassa. Edelleen signaalitiedustelun rakenteen ja toiminnan katsotaan olevan EIT:n ratkaisussa suhteellisia järjestelmän tarkoituksen saavuttamiseksi.

Tietoliikennetiedustelun edellytyksenä oleva välttämättömyys on luettava myös osana esitetyn lain kokonaisuutta. On huomattava, että jo poliisilain 1 luvun yleisistä periaatteista seuraa useita tiedustelumenetelmien käytön rajoituksia (periaatteiden merkitystä tiedustelumenetelmien käytössä käsitelty myös HE 202/2017 vp., s. 169–170).

6.2 Tietolähteen turvaaminen siviilitiedustelussa (Poliisilaki 5 a luku 25 §)

Eduskunnan oikeusasiamies katsoo, että tietolähteelle annettavien henkilötietojen käyttö voisi tarkoittaa tosiasiallisesti peitetoimintaa, minkä vuoksi sitä ei voida käyttää tiedustelutiedon hankkimiseksi vaan ainoastaan tiedonhankinnan jälkeen tietolähteen turvaamiseksi. Eduskunnan oikeusasiamiehen mukaan tämän tulisi käydä ilmi pykälätekstistä.

KRP katsoo, että erityisesti 5 momentin mukaisten suojaamiskeinojen käyttäminen tiedonhankinnan yhteydessä voi muuttaa tiedonhankintakeinon luonteeltaan kokonaan toisenlaiseksi. Ainakin niissä tilanteissa, joissa vääriä rekisterimerkintöjä ja asiakirjoja käytetään osana tietolähteen ohjattua käyttöä, kyse on tosiasiallisesti siviilihenkilöiden toteuttamasta peitetoiminnasta.

Sisäministeriön vastaus: Pykälän tarkoituksena on sen nimen mukaisesti tietolähteen turvaaminen, jolla tarkoitetaan tietolähteen hengen ja terveyden turvaamista tietojen antamisen aiheuttamalta uhalta. Tietolähteen turvaamisen ydintarkoituksena ei ole tiedonhankinta, vaan sen fuktio on toissijainen, tiedonhankinnan mahdollistava.

Suojelupoliisilla on lähtökohtaisesti velvollisuus huolehtia tietolähteidensä turvallisuudesta tarpeen mukaan tiedonhankinnan aikana ja sen jälkeen, mutta myös ennen tiedonhankinnan alkamista, jos tietolähteen tiedetään antavan kansallisen turvallisuuden kannalta merkityksellisiä tietoja. Tietolähteen turvaamistoimivaltuus ei kuitenkaan korvaise todistajansuojeluohjelmasta annetussa laissa (88/2015) tarkoitettua todistajansuojeluohjelmaa. Jos tietolähdettä olisi tarpeen suojella pidempiaikaisesti ja häneen kohdistuisi vakava hengen tai terveyden uhka eikä uhkaa voitaisi tehokkaasti torjua muilla toimenpiteillä, niin olisi perusteltua harkita tietolähteen kohdalla todistajansuojeluohjelman käynnistämistä.

Pykälän 5 momentissa säädettäisiin tietolähteen hengen ja terveyden suojaamisesta. Tietolähteen turvaamisessa olisi kyse tietolähteelle lyhytaikaisesti luotavasta peitehenkilöllisyydestä väärien,

harhauttavien tai peiteltyjen tietojen tai rekisterimerkintöjen taikka väärin asiakirjojen avulla. Momentin tarkoittamassa tilanteessa olisi toissijaisesti kyse tietolähteen hallussa olevien tietojen toimittamisen turvaamisesta. Väliaikaisen peitehenkilöllisyyden luomisen edellytyksenä olisi, että toimenpiteen on oltava välttämätön tietolähteen hengen ja terveyden suojaamiseksi.

Tietolähteen turvaaminen voisi tulla kyseeseen esimerkiksi tilanteessa, jossa tietolähteellä olisi hallussaan erittäin tärkeitä tietoja kansallista turvallisuutta vakavasti uhkaavasta toiminnasta eikä tietoja voitaisi toimittaa suojelupoliisille muutoin kuin tapaamalla tietolähde henkilökohtaisesti. Erona rikostorjunnassa käytettyjen (ohjattujen) tietolähteiden suojaamiseen tai turvaamiseen, siviilitiedustelussa merkitykselliset tietolähteet ovat Suomen rajojen ulkopuolella tai muutoin toisen valtion suvereniteetin piirissä. Ulkomailla oleva Suomeen pyrkivä tietolähde joutuu poikkeuksetta niin oman kuin Suomen valtion rajamuodollisuuksien kohteeksi. On ilmeistä, että Suomeen pääseminen voi edellyttää lyhytaikaisen peitehenkilöllisyyden luomista tietolähteelle.

Rekisterimerkintä olisi oikaistava sen jälkeen, kun tässä momentissa tarkoitettuja edellytyksiä ei enää ole. Esimerkiksi, kun Suomeen pyrkivä tietolähde olisi päässyt Suomeen eikä tietolähteen henki ja terveys olisi vaarassa, niin peitehenkilöllisyyttä koskevat tiedot olisi korjattava ja väärät asiakirjat olisi otettava pois tietolähteeltä.

Tietolähteen turvaaminen ei käytännössä mahdollistaisi peitetointia. Peitetointin toteuttaminen reaali maailmassa edellyttää käytännössä pitkäaikaisen historian luomista peitehenkilölle

Jos olisi syytä epäillä tietolähteen luotettavuutta, niin jo ennen tietolähteen turvaamistoimiin ryhtymistä voisi olla tarpeen selvittää tietolähteen luotettavuus. Tietolähteeseen voitaisiin tiedustelumenetelmien käyttöedellytysten täytyessä kohdistaa tiedonhankintaa muun muassa sen varmistamiseksi, että kyseessä on tietolähde, keneltä on syytä olettaa saatavan tietoja toiminnasta, joka vakavasti uhkaa Suomen kansallista turvallisuutta.

6.3 Paikkatiedustelun kohde

Eduskunnan oikeusasiamies toteaa, että siviilitiedustelua koskevan esityksen perusteluissa on sivulla 200 todettu, että kysymys on uskonnonvapauslaissa tarkoitetun rekisteröidyn uskonnollisen yhdyskunnan papin tiloista. Taustalla on oikeudenkäymiskaaren 17 luvun 16 §:ssä tarkoitettu rippisalaisuus. Käsitykseni mukaan tämä ei voine tarkoittaa esimerkiksi kirkkosalia.

Sisäministeriön vastaus: Poliisilain 5 luvun 26 §:ssä ehdotetaan säädettäväksi paikkatiedustelun määritelmästä. Pykälän mukaan paikkatiedustelulla tarkoitetaan muussa kuin vakituiseen asumiseen käytettävässä paikassa tai sellaisessa paikassa, jossa tiedustelun kohteeksi on syytä olettaa joutuvan tietoa, josta oikeudenkäymiskaaren 17 luvun 11, 13, 14, 16, 20, 21 §:n tai 22 §:n 2 momentin mukaan on velvollisuus tai oikeus kieltäytyä todistamasta, toimitettavaa tiedustelua esineen, omaisuuden, asiakirjan, tiedon tai seikan löytämiseksi. Päätös paikkatiedustelun kohteesta perustuu aina tapauskohtaiseen harkintaan. Jos paikkatiedustelun aikana ilmenee, että tiedustelu on kohdistunut tietoon, josta oikeudenkäymiskaaren 17 luvun 11, 13, 14, 16, 20, 21 §:n tai 22 §:n 2 momentin mukaan on velvollisuus tai oikeus kieltäytyä todistamasta, on tiedustelu siltä osin heti lopetettava ja tietoa koskevat muistiinpanot ja jäljennökset heti hävitettävä.

6.4 Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen (Poliisilaki 5 a luku 16 §)

FiCom, Ficix, CSC, Elisa Oyj, DNA Oyj ovat kiinnittäneet huomiota poliisilain muuttamista koskevan lakiehdotuksen 5 a luvun 16 §:ään, jossa ehdotetaan säädettäväksi laitteen, menetelmän tai ohjelmiston asentamisesta ja poisottamisesta siviilitiedustelussa. Lausunnonantajat katsovat, ettei tiedusteluviranomaisella tulisi olla pääsyä teleyritysten tai tietoyhteiskunnan palvelujen tarjoajien laitteisiin.

Sisäministeriön vastaus: Sisäministeriö toteaa, että lausunnonantajien huomiot ovat perusteltuja, vaikka tilanteet olisivatkin erittäin harvinaisia Suomessa.

Todettakoon, että hyvin vastaavatyypinen säännös on voimassa olevan poliisilain 5 luvun 26 §:ssä, joka koskee teknisen tarkkailun menetelmiä. Ehdotettavan 5 a luvun 16 §:n asentamistoimivaltuutta esitetään poliisilain 5 luvun 26 §:stä poiketen laajennettavaksi myös telekuunteluun, tietojen

hankkimiseen telekuuntelun sijasta sekä televalvontaan. Tässä suhteessa on syytä huomioida, että telekuuntelun, tietojen hankkimisen telekuuntelun sijasta sekä televalvonnan kohdalla asentamistoimivaltuuden käyttäminen tulisi lähtökohtaisesti sovellettavaksi ulkomaan tiedustelussa. Tämä johtuu muun muassa siitä, että on hyvin epätodennäköistä, että ulkomainen teleyritys avustaisi suojelupoliisia tarvittavien kytkentöjen tekemisessä. Asioiminen kohdevaltiossa toimivan teleyrityksen kanssa myös aiheuttaisi merkittävän paljastumisriskin.

Sisämaassa käytettävien toimivaltuuksien käytössä toimittaisiin vastaavasti, kuten nykyisten poliisilain 5 luvussa tarkoitettujen telekuuntelun, tietojen hankkimisen telekuuntelun sijasta sekä televalvonnan kohdalla. Tiedusteluviranomainen hakisi luvan tuomioistuimelta mainittujen toimivaltuuksien käyttämiseksi. Jos tiedustelumenetelmän käytöstä päättäisi tuomioistuin, niin myös tiedustelumenetelmän käyttöä koskevassa luvassa tulisi erikseen sallia laitteen, menetelmän tai ohjelmiston asentaminen. Näin ollen asentamistoimivaltuutta sovellettaessa tuomioistuinmenettelyssä tulisi yksittäistapauksellisesti myös arvioitavaksi toimivaltuuden toteuttamisen tapa. Asiassa on syytä korostaa sitä, ettei esimerkiksi telekuuntelua tai televalvontaa saisi kiertää käyttämällä teknisen tarkkailun toimivaltuuksia, vaan suojelupoliisi saa käyttää toimivaltuuttaan vain säädettyyn tarkoitukseen (tarkoitussidonnaisuuden periaate).

Laitteen, menetelmän tai ohjelmiston asentamisen ja poisottamisen yhteydessä tulisi aina pohtia sen mahdollisesti aiheuttamaa kiinnijäämisriskiä sekä myös asentamisen kohteelle aiheutuvaa mahdollista vahingon riskiä. Esimerkiksi salaa tietojärjestelmään asennettu teknisen laitetarkkailun ohjelmisto sisältää aina mahdollisen riskin tietojärjestelmän toiminnalle ja on omiaan heikentämään sen turvallisuutta. Suojelupoliisin toimenpiteillä ei saisi aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä laitteen, menetelmän tai ohjelmiston asentamisen ja poisottamisen yhteydessä (vähimmän haitan periaate).

Poliisilain muuttamista koskevan lakiehdotuksen 5 a luvun 51 §:ssä ehdotetaan säädettäväksi teleyrityksen velvollisuus avustaa siviilitiedustelussa ja 55 §:ssä yhteistyöstä yhteisöjen kanssa. Jälkimmäisen pykälän 1 momentin mukaan suojelupoliisin on tarpeen mukaan toimittava yhteistyössä muiden viranomaisten kanssa siviilitiedustelun tarkoituksenmukaiseksi hoitamiseksi. Tämä voi tarkoittaa esimerkiksi suojelupoliisille ja teleyrityksille yhteisesti hyväksyttävien toimintatapojen ja -käytänteiden laatimista.

6.5 Lupa-aika 6kk

Eduskunnan oikeusasiamies kiinnittää huomioita siihen, että monissa ehdotetuissa tiedustelumenetelmissä lupa voidaan antaa jopa kuusi kertaa pidemmäksi ajaksi (1kk/6kk) kuin mitä samaa keinoa voidaan käyttää salaisessa tiedonhankinnassa (5 a luvun 6 §, 7 §, 11 §, 12 §, 14 §, 20 §).

Helsingin käräjäoikeus toteaa lausunnossaan, että myös tiedustelumenetelmiä koskevan poliisilain 5a luvun 3 §:ssä tarkoitetuissa on ainakin pääsääntöisesti kysymys hyvin pitkäjänteisestä toiminnasta, joka tapahtuu salaisesti, vähitellen ja pitkän ajan kuluessa. Myös tiedustelumenetelmiä hyväksi käyttämällä saatava tieto koostuu todennäköisesti samalla tavalla ennemminkin pitkän ajan kuluessa kertyvistä palasista kuin yksittäisistä yksiselitteisistä tiedoista. Mikäli lupa voitaisiin myöntää vain esimerkiksi kuukaudeksi, vaarana olisi jatkohakemusten ketjuuntuminen lukuisiksi kuukauden välein tapahtuviksi käsittelyiksi samalla kun kunkin käsittelyn yhteydessä saatavan uuden tiedon määrä saattaisi jäädä hyvinkin vähäiseksi. Mikäli tiedustelumenetelmän käytölle sen sijaan tarvitaan kuuden kuukauden jälkeen jatkoa, uusi käsittely antaa myös tuomioistuimelle aidon mahdollisuuden kontrolloida luvan edellytysten olevan edelleen olemassa. Harva käsittelyrytmi palvelee siis oikeusvarmuutta ja samalla lisäksi osaltaan myös asioiden salassa pitämisen tarvetta. Koska lupa voidaan myöntää enintään kuudeksi kuukaudeksi, sekä luvanhakijalla että tuomioistuimella on mahdollisuus arvioida luvan kesto

Sisäministeriön vastaus: Poliisilain 5 a luvussa ehdotettujen tiedustelumenetelmien lupa voidaan antaa useiden tiedustelumenetelmien kohdalla kuuden kuukauden pituiseksi ajaksi. Pidempi lupa-aika on perusteltu siviilitiedustelun luonteen ja tiedustelumenetelmien käytön perusteen vuoksi. Tiedustelutoiminnan luonne poikkeaa merkittävästi rikostorjunnan tarpeista. Jos tiedustelumenetelmän käytölle tarvittaisiin kuuden kuukauden jälkeen jatkoa, uusi käsittely antaisi myös tuomioistuimelle aidon mahdollisuuden kontrolloida luvan edellytysten olevan edelleen olemassa vaarantamatta oikeusturvaa. Todettakoon, että rikostorjuntatoimivaltuuksien osalta suunnitelmallista tarkkailua,

teknistä seuranta- ja peitetoimintaa ja tietolähteen ohjattua käyttöä koskevat päätökset voidaan jo nykyisin tehdä kerrallaan enintään kuudeksi kuukaudeksi.

Siviilitiedustelua koskevassa hallituksen esityksessä tarkoitettu koskeva kuuden kuukauden lupa-aika ei automaattisesti tarkoittaisi sitä, että lupa voitaisiin aina hakea kuudeksi kuukaudeksi tai että se tulisi myöntää kuuden kuukauden määräajaksi. Suhteellisuus- ja vähimmän haitan periaatteen mukaista harkintaa edellyttäisi säännöksessä oleva ilmaisu ”enintään kuudeksi kuukaudeksi kerrallaan”. Siksi lupaa haettaessa sekä sitä myönnettäessä tulisi harkita tiedustelumenetelmän käytön ajallisen keston tarpeellisuutta tapauskohtaisesti. Tämä antaisi enemmän harkintavaltaa tuomioistuimelle ja palvelisi samalla oikeusvarmuutta.

Tiedustelu on rikostorjuntaan verrattuna usein pidempikestoisempaa ja operaatiot ennakkoon tarkoin suunniteltuja. Operaation tavoitteena voi olla esimerkiksi kerätä tietoa kohdevaltion Suomen etuja vahingoittavasta toiminnasta ja siihen liittyvistä seikoista. Jos tiedusteluoperaation kohde on merkittävä, sen kesto voi olla hyvinkin pitkäaikaista. Näin tarkoituksena ei ole yksittäisen rikoksen estäminen tai selvittäminen, vaan varhaisen vaiheen tiedon kerääminen kokonais kuvan saamiseksi. Säännös mahdollistaisi näin ollen ennakoivan ja pidempiaikaisemman tiedonhankinnan yhdellä lupapäätöksellä.

EIT on ratkaisukäytännössään ottanut kantaa kuuden kuukauden lupa-aikaan muun muassa ratkaisussa *Zakharov v. Venäjä* sekä kesäkuussa annetussa ratkaisussa *Centrum för Rättvisa v. Ruotsi*. *Zakharov v. Venäjä* on merkittävä siksi, että EIT siinä otti kantaa paitsi Venäjän lain muodolliseen sisältöön, myös laajasti lain käytännön soveltamiseen. Ratkaisu koski Venäjän sisäisen turvallisuuspalvelu FSB:n omasta puolestaan ja muiden viranomaisten toimeksiannosta harjoittamaa posti-, tele- ja muun viestiliikenteen valvontaa, josta oli säädetty kansallisessa laissa. Laki määritteli tarkkailutoimenpiteiden maksimaaliseksi kestoksi kuusi kuukautta, mitä tuomioistuin piti sinänsä asianmukaisena. Laissa ei kuitenkaan säädetty, että toimivaltuuden käyttö oli lopetettava ennen määräajan päättymistä, jos käytön edellytykset eivät enää täyttyneet.

Centrum för Rättvisa v. Ruotsi ratkaisussa EIT katsoi, ettei tiedustelumenetelmien käytön tarkasta kestosta välttämättä tarvitse säätää lainsäädännössä, kunhan tämän arvion suorittavat pätevät viranomaiset. Tämän lisäksi edellytyksenä ovat riittävät kansallisessa laissa olevat suojakeinot, kuten ajankohta jonka jälkeen lupa vanhenee, olosuhteet joissa lupa voidaan uusida ja olosuhteet joissa se tulee perua. Ruotsin lainsäädännössä kaksi ensimmäistä suojakeinoa ovat selvästi havaittavissa signaalitiedustelulaissa: Lupa myönnetään kuudeksi kuukaudeksi kerrallaan, jonka jälkeen suoritetaan täysmittainen arvio siitä, voidaanko lupa uusida. Perumisen osalta Ruotsin lainsäädäntö ei ole yhtä tarkkaa. EIT kuitenkin katsoi, että erilaiset valvovat elimet kuten tiedusteluvaltuusto toimivat riittävänä takeena sille, että virheelliset luvat peruutetaan.

Todettakoon, että Suomeen ehdotettu lainsäädäntö olisi paikoin tiukempi kuin Ruotsin vastaava.

Sekä siviilitiedustelua että sotilastiedustelua koskevissa hallituksen esityksissä ehdotetaan lupaviranomaiseksi Helsingin käräjäoikeutta. Tämä on saanut myös kannatusta esityksistä annetuissa lausunnoissa. Helsingin käräjäoikeudella on maan laajin kokemus salaisten tiedonhankinta- ja pakkokeinoasioiden käsittelemisestä. Erikoisosaamisen tarve on mahdollista saavuttaa keskittämällä tiedustelumenetelmiä koskevat lupa-asiat sille.

6.6 Kansainvälinen yhteistyö

Eduskunnan ulkoasiainvaliokunta katsoo lausunnossaan, että asiaa koskevan pykälän kirjaus on muodoltaan hyvin yleisluonteinen, ja valiokunta toteaa kirjausten perusteella olevan mahdollista arvioida, miten ihmisoikeussopimuksiin liittyviä velvoitteita tullaan soveltamaan tiedustelutoiminnan kansainvälisen yhteistyön yhteydessä. Valiokunta pitää tärkeänä selvittää ao. pykälän perusteluissa, että lauseke kieltää yhteistoiminnan tai tietojen luovuttamisen, jos on perusteltua aihetta epäillä, että ketään henkilöä tämän yhteistyön tai tietojen luovuttamisen vuoksi uhkaa kuolemanrangaistus, kidutus, muu ihmisarvoa loukkaava kohtelu, vaino, mielivaltainen vapaudenriisto tai epäoikeudenmukainen oikeudenkäynti.

Professori Olli Mäenpää katsoo, että tiedustelutoiminnassa kansainvälinen yhteistyö on pääasiassa voimavara, joka vahvistaa kansallisten viranomaisten toimintaedellytyksiä. Tältä kannalta voidaan keskeisenä toimivaltaperusteena pitää 5 a luvun 57 §:n säännöstä, jonka mukaan suojelupoliisi voisi luovuttaa myös salaisia tietoja kansainvälisessä yhteistyössä, jos tietojen luovuttaminen on tarpeen

kansallisen turvallisuuden suojaamiseksi eikä tietojen luovuttaminen ole vastoin kansallista etua. Sääntely on tältä osin hyvin väljää, mutta sen voitaneen arvioida vastaavan tiedustelutoiminnan kansainvälisen yhteistyön välttämättömiä tarpeita.

Ihmisoikeusliitto ja **Effi ry** kiinnittävät huomiota kansainvälisen yhteistyön sääntelyn epämääräisyyteen ja siihen, että kansainvälistä yhteistyötä koskevaan pykälään olisi tarpeellista lisätä velvoite ihmisoikeuksien kunnioittamisesta.

Sisäministeriön vastaus: Siviilitiedustelulainsäädännön yhteydessä ehdotetaan henkilötietojen käsittelystä poliisitoimessa annettua lakia muutettavaksi ainoastaan välttämättömiltä osilta, koska poliisin henkilötietojen käsittelyä koskevan lainsäädännön kokonaisuudistus on vireillä. Jälkimmäisellä esityksellä uudistetaan voimassa oleva henkilötietojen käsittelystä poliisitoimessa annettu laki poliisitoiminnan tarpeet huomioon ottaen. Säännöksissä huomioidaan Euroopan unionin tietosuojalainsäädännön vaatimukset. Kyseisen hankkeen on tarkoitus edetä eduskuntaan kuluvan vuoden aikana. Henkilötietojen käsittelystä säädetään siis tässä yhteydessä, kun siviilitiedustelulainsäädännön kohdalla kyse on pääsääntöisesti muiden tietojen käsittelystä.

Näin ollen siviilitiedustelulainsäädännössä tarkoitettu tietojen luovuttaminen koskisi muita tietoja kuin henkilötietoja, joiden luovuttamisen perusteena tulisi olemaan "välttämättömyys". On myös huomattava, ettei tiedustelutoiminnassa tiedonhankinnan keskiössä ole aina yksittäiset henkilöt, vaan tietoja vaihdetaan myös valtioiden ja muunlaisten ryhmittymien suunnitelmista, niiden taktisesta ja operatiivisesta toiminnasta sekä resursseista.

Tietojen luovuttamisessa ja osallistumisessa yhteiseen tiedusteluoperaatioon vieraan valtion kanssa olisi aina oltava Suomen etujen mukaista. Tällä tarkoitettaisiin kaikkia sellaisia seikkoja, jotka saattaisivat huonontaa Suomen kansallista etua. Suomen edun mukaista ei lähtökohtaisesti olisi luovuttaa vieraan valtion tiedusteluviranomaiselle esimerkiksi tietoja suomalaisten yritysten yrityssalaisuuksista tai muita tietoja, jotka voisivat esimerkiksi heikentää Suomen alueella oleskelevien perus- ja ihmisoikeuksia.

Voimassa olevan poliisilain 1 luvussa säädetään poliisia, myös suojelupoliisia, velvoittavista poliisioikeudellisista periaatteista. Poliisilain 1 luvun 2 §:n mukaan: "Poliisin on kunnioitettava perusoikeuksia ja ihmisoikeuksia sekä toimivaltuuksia käyttäessään valittava perusteltavissa olevista vaihtoehdoista se, joka parhaiten edistää näiden oikeuksien toteutumista." Kyseinen lainkohta koskee kaikkea suojelupoliisin toimintaa.

Suomen perustuslain 22 §:ssä säädetään, että julkisen vallan on turvattava perusoikeuksien ja ihmisoikeuksien toteutuminen. Euroopan ihmisoikeussopimuksen 3-5 artikloissa määrätään kidutuksen kiellosta, orjuuden ja pakkotyön kiellosta, oikeudesta vapauteen ja turvallisuuteen. Vastaavanlaisia ihmisoikeusmääräyksiä ilmenee useita ylikansallisista Suomea velvoittavista sopimuksista.

Sisäministeriö ei katso tarpeelliseksi säätää nimenomaista ihmisoikeuksien kunnioittamisen lausumaan kansainvälisen yhteistyön pykälään, koska tämä velvoite tulee jo useasta eri perustuslainkohdasta sekä eduskuntalainvoimalla olevasta oikeussäännöstä.

7 Tiedusteluvaltuutetun rooli tuomioistuimessa

Oikeuskansleri katsoo, että Helsingin käräjäoikeuden, joka keskitetysti käsittelee tiedusteluvaltuuksia koskevia asioita, resursseihin ja asiantuntemukseen ja muihin toimintaedellytyksiin on tärkeää kiinnittää huomiota. TuomioistuINVALVONNASSA saattaisi olla aihetta voida myös kuulla tiedusteluvaltuutettua asiantuntijana.

KKO, Effi ry ja Amnesty kiinnittävät lausunnoissaan huomiota tiedusteluvaltuutetun rooliin tiedustelumenetelmiä koskevassa tuomioistuimen lupakäsittelyssä. Tiedusteluvaltuutetulle esitetty rooli olisi tiedustelutoiminnan valvonnasta annetun hallituksen esityksen (HE 199/2017 vp) mukaan passiivinen eikä tiedusteluvaltuutetulle ole varattu oikeutta käyttää puhevaltaa lupakäsittelyssä. Lausunnonantajat kannattavat tiedusteluvaltuutetulle aktiivisempaa roolia.

KKO pitää selvänä puutteena sitä, ettei tiedusteluvaltuutetulla kuitenkaan olisi asianosaisen asemaa oikeudenkäynnissä, jossa tiedusteluviranomainen hakee tuomioistuimelta lupaa tiedustelumenetelmän käyttöön, että tiedusteluvaltuutetun vahva rooli lupaprosessissa syventäisi ja monipuolistaisi

tuomioistuimen harkintaa lupa-asioissa. Tiedusteluvaltuutetun aktiivinen osallistuminen ainakin niihin lupaoikeudenkäynteihin, joissa linjataan uudenlaisia tiedustelutilanteita, tasoittaisi myös sitä asiantuntemuksen eroa, joka tuomioistuimen ja tiedusteluviranomaisten välillä ymmärrettävästi on.

KKO katsoo lausunnossaan, että tuomioistuinten riippumattomuuden vuoksi oikeana lähtökohtana on, että tiedusteluvaltuutetun toimivaltaan ei kuuluisi tuomioistuihin kohdistu laillisuusvalvonta.

Helsingin käräjäoikeus katsoo lausunnossaan, että tiedusteluvaltuutetun läsnäolo-oikeus ohjaa osaltaan tiedusteluluvan hakijaa riittävien perustelujen esittämiseen tiedustelumenetelmän käyttöluvahakemuksessa.

Sisäministeriön vastaus: Tiedustelutoiminnan valvontalain 14 §:ssä ehdotetaan säädettäväksi tiedusteluvaltuutetun läsnäolo-oikeudesta tuomioistuimessa. Tiedusteluvaltuutetun läsnäolo-oikeus koskisi siviili- ja sotilastiedustelumenetelmien lupakäsittelyä Helsingin käräjäoikeudessa. Tämän lisäksi valtuutetulla olisi oikeus olla läsnä tällaisessa lupa-asiassa annettuun päätökseen tehdyn kantelun käsittelyssä Helsingin hovioikeudessa.

Läsnäolo-oikeudella turvattaisiin tiedusteluvaltuutetun mahdollisuus saada tietoonsa reaaliaikaisesti kaikki tuomioistuinkäsittelyssä esillä olevat seikat tiedustelumenetelmän käytön perusteista ja edellytyksistä. Käytännössä osa lupahakemuksen tueksi esitetyistä seikoista annetaan tuomioistuimelle suullisesti. Valtuutetun tiedonsaantioikeus täydentyisi tämän läsnäolo-oikeuden kautta eikä tiedusteluvaltuutettua olisi suljettu pois mistään tiedustelumenetelmäprosessin vaiheesta. Läsnäolo-oikeus myös ohjaisi osaltaan tiedusteluluvan hakijaa riittävien perustelujen esittämiseen tiedustelumenetelmän käyttöluvahakemuksessa (HE 199/2017 vp, s. 58).

Tiedusteluvaltuutettu voi myös ennakkollisesti tiedonsaantioikeuksien (valvontalakiehdotuksen 8 §) nojalla tutustua suojelupoliisin aineistoon ennen suojelupoliisin tuomioistuimelle esittämää lupavaatimusta. Lisäksi tiedusteluvaltuutettu voi luvan myöntämisen jälkeen vielä varmistua siitä, että suojelupoliisi on toiminut lainmukaisesti lupavaatimusta esittäessään ja että suojelupoliisi on toimittanut Helsingin käräjäoikeudelle riittävät ja oikeat tiedot lupaharkintaa varten. Tiedusteluvaltuutetulle ehdotetaan poikkeuksellisen vahvoja laillisuusvalvojan toimivaltuuksia ja se voi määrätä tiedustelumenetelmän käytön keskeytettäväksi tai lopetettavaksi, jos hän katsoo valvottavan menetelleen lainvastaisesti tiedustelutoiminnassa (valvontalakiehdotuksen 15 §).

Tiedusteluvaltuutetun läsnäolo-oikeudessa ei olisi kyse tuomioistuimen toiminnan valvonnasta. Läsnäolo-oikeus sisältäisi oikeuden saapua paikalle tuomioistuimen istuntoon tai oikeuden osallistua paikallaoloa vastaavalla tavalla teknistä tiedonvälitystapaa käyttäen pidettävään tuomioistuinkäsittelyyn. Läsnäolo-oikeus tarkoittaisi valtuutetun oikeutta kuunnella ja katsoa kaikki käsittelyssä esitettävä aines. Läsnäolo-oikeuteen ei sisältyisi muita osallistumisoikeuksia tuomioistuinkäsittelyyn kuten oikeutta tulla kuulluksi tai esittää muutoin näkemyksiään istunnossa (HE 199/2017 vp, s. 58).

Tiedusteluvaltuutetun roolin vahvistaminen niin, että tämä toimisi lupakäsittelyssä parttina tai valtuutetun puhevallan lisääminen olisi poikkeuksellinen ratkaisu. Tämänlainen roolin vahvistaminen johtaisi tiedusteluvaltuutetun puolueettomuuden vaarantumiseen tiedustelutoiminnan ulkoisena laillisuusvalvojana. Jos tiedusteluvaltuutettu toimisi parttina tai voisi käyttää puhevaltaa tuomioistuin käsittelyssä, niin käytännössä tiedusteluvaltuutettu osallistuisi tiedustelumenetelmän käyttöä koskevaan päätöksentekoon, mikä ei ole laillisuusvalvojan tehtävänä. Käytännössä voisi muodostua tilanne, jossa Helsingin käräjäoikeus tekisi tiedusteluvaltuutetun näkemyksen vastaisen ja valtuutetun kannalta kielteisen ratkaisun. Tämä saattaisi johtaa tilanteeseen, jossa tiedusteluvaltuutettu voisi itse toimia eräänlaisena valitusinstanssina itselleen.

8 Ilmoitus syyttäjälle poliisirikoksista

Valtakunnansyyttäjänvirasto toteaa, että tiedustelutoiminnassa havaitut poliisimiehiä koskevat rikokset olisi aina ilmoitettava syyttäjälle riippumatta, mikä mahdollisen rikoksen rangaistusasteikko on. Valtakunnansyyttäjänvirasto pitää tarkoituksenmukaisena sitä, että suojelupoliisi ilmoittaisi syyttäjän toimivaltaan kuuluvat asiat suoraan Valtakunnansyyttäjänvirastolle. Valtakunnansyyttäjänvirasto toteaa, että 5 momentin sanamuodon mukaan tämä velvollisuus ei koskisi syyttäjää, koska syyttäjä ei ole esitutkintaviranomainen eikä myöskään muu lainkohdassa tarkoitettu viranomainen.

Sisäministeriön vastaus: Esitutkintalain 5 luvun 1 §:ssä säädetään ilmoituksen tekemisestä syyttäjälle. Pykälän mukaan esitutkintaviranomaisen on viipymättä ilmoitettava syyttäjälle asiasta, jossa rikoksesta epäiltynä on poliisimies, jollei asiaa käsitellä sakon ja rikesakon määräämisestä annetussa laissa säädettyssä menettelyssä. Syyttäjälle on lisäksi ilmoitettava tutkittavaksi tulleesta rikoksesta, jonka esitutkinta- ja syyttäväviranomaiset ovat yhdessä niille kuuluvan toimivallan perusteella päättäneet kuuluvan ilmoitusvelvollisuuden piiriin tai josta syyttäjä on pyytänyt ilmoittamaan.

Asiassa on syytä huomioida, ettei suojelupoliisi olisi enää jatkossa esitutkintaviranomainen eikä kyseinen esitutkintalain sääntely enää koskisi suojelupoliisin toimintaa. Poliisilain 5 a luvun 44 §:ssä ehdotetaan säädettäväksi siviilitiedustelussa saadun tiedon luovuttaminen rikostorjuntaan eli ns. palomuurista. Siinä ei ole erikseen huomioitu poliisirikosasioita, koska myös niiden osalta on katsottu riittäväksi menettelyksi mitä pykälässä ehdotetaan säädettäväksi.

Palomuri on rakennettu siten, että ylitörkeistä rikoksista ja rikoksista, joista säädetty ankarin rangaistus on vähintään kolme vuotta vankeutta, toimitaan yhden luukun periaatteen mukaan ja ilmoitus tehdään keskusrikospoliisille. Keskusrikospoliisi tekee ilmoituksen tämän jälkeen toimivaltaiselle taholle ja toimittaa tarvittavat tiedot ilmoituksen yhteydessä. Jos kyse on poliisirikosasiasta, niin ilmoitus tulee ETL 5:1:n mukaan tehdä syyttäjälle.

Kaikissa tilanteissa ei aina ole helposti todennettavissa, että rikoksenteijänä on poliisi. Kuten normaalistikin poliisin ulkopuolisen henkilön havaitessa rikoksen, ensisijaisesti siitä ilmoitetaan poliisille, joka poliisia velvoittavan lainsäädännön nojalla siirtää esitutinnan johtovastuun syyttäjälle ja esitutkinta suoritetaan eri poliisiyksikössä kuin se, missä rikoksesta epäilty toimii.

Jos eduskunta katsoo, että poliisirikosasioissa suojelupoliisilla tulisi olla ehdoton ilmoitusvelvollisuus suoraan syyttäjälle, niin asiasta on mahdollista säätää seuraavasti:

Poliisilaki 5 a luku 44 §:ään uusi momentti

"Jos tiedustelumenetelmän käytön aikana ilmenee, että poliisimiestä on syytä epäillä rikoksesta, suojelupoliisin tekemään ilmoitukseen sovelletaan mitä esitutkintalain 5 luvun 1 §:ssä säädetään esitutkintaviranomaisen tekemästä ilmoituksesta syyttäjälle."

9 Kansallisen turvallisuuden käsite

Eduskunnan oikeusasiamies toteaa lausunnossaan, että siviilitiedustelu ei ole rikosperusteista, vaan siinä on kyse huomattavasti epämääräisemmästä ilmiö- tai uhkaperusteisesta tiedonhankinnasta. Tiedustelumenetelmän käytön yleisenä edellytyksenä on, että sillä voidaan perustellusti olettaa saatavan tietoja sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Kansallisen turvallisuuden käsitesisältö on varsin epämääräinen eikä sitä ole laissa tarkemmin määritelty. Tämän vuoksi ehdotettujen tiedustelumenetelmien käyttöedellytykset ja niiden kohdentaminen on hyvin väljää verrattuna samojen keinojen käyttöön salaisessa tiedonhankinnassa.

Sisäministeriön vastaus: Kuten eduskunnan oikeusasiamies lausunnossaan toteaa, niin salaisten tiedonhankintakeinojen käyttöperusteille yhteinen piirre on se, että ne on määritelty henkilö- ja rikoslähtöisesti. Niitä voidaan kohdistaa vain henkilöön tai käyttää hankittaessa tietoa vain sellaisen henkilön toiminnasta, jonka voidaan perustellusti olettaa tulevaisuudessa syyllistyvän tai jo syyllistyneen tietyn rangaistusuhan täyttävään rikokseen tai sellaisen valmisteluun.

Salainen tiedonhankinta tulisi mahdollistaa rikostorjuntatoimivaltuuksien lisäksi sellaisen toiminnan kohdalla, joka vakavasti uhkaa Suomen kansallista turvallisuutta joko suoraan tai välillisesti. Kansallista turvallisuutta vakavasti uhkaava toiminta voi olla sellaista, joka konkretisoituessaan voisi muodostua rikokseksi, mutta johon ei vielä voida kohdistaa konkreettista ja yksilöityä rikosepäilyä. Samoin kyse voi olla toiminnasta, joka ei ole Suomen lain mukaan rikos eikä voisi sellaiseksi muodostuakaan. Lisäksi kyse voi olla kansallista turvallisuutta vakavasti uhkaavasta toiminnasta, joka tapahtuu ulkomailla eikä toiminnasta voida nykyisillä toimivaltuuksilla hankkia tietoa.

Tiedon hankkimisen tulisi sisältää myös Suomeen kohdistuvien ulkoisten uhkien kartoittamisen. Kyse olisi siten esimerkiksi turvallisuusympäristön kehityksen seuraamisesta kansalliseen turvallisuuteen kohdistuvan tilannekuvan muodostamiseksi. Ilmaisuu kattaasi myös jatkuvan tiedonhankinnan kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. Tiedonhankintaa ei siten olisi rajoitettu

ajallisesti, sillä tiedustelutoimintaa on usein tarpeen seurata pitkäjänteisesti ja systemaattisesti ilman, että seurattavan toiminnan välttämättä tarvitsisi olla välittömästi uhkaavaa seurannan aikana.

Perustuslain muuttamista koskevassa hallituksen esityksessä (HE 198/2017 vp) ehdotetaan perustuslain 10 §:ää muutettavaksi niin, että lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten torjunnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Ilmaisia ”kansallinen turvallisuus” käytetään jo nykyisessä lainsäädännössä. Se esiintyy myös Euroopan unionin oikeusjärjestyksessä ja kansainvälisissä ihmisoikeussopimuksissa ihmisoikeuksien rajoitusperusteena. Käsitteelle ei ole annettu sen yleiskielen merkitystä tarkempaa sisältöä unionin oikeusjärjestyksessä tai ihmisoikeusvelvoitteissa. Esimerkiksi Euroopan ihmisoikeussopimuksen tulkinnassa valtioilla on katsottu olevan varsin laaja harkintamarginaali sen suhteen, millaisen toiminnan ne katsovat vaarantavan kansallista turvallisuuttaan (esim. Kennedy v. Yhdistynyt Kuningaskunta, 18.5.2010). Euroopan ihmisoikeustuomioistuin on kuitenkin asettanut salaisia tiedonhankintamenetelmiä koskevalle lainsäädännölle vähimmäisvaatimuksia, joiden tarkoituksena on estää mielivaltainen puuttuminen yksilön luottamuksellisen viestin suojaan (esim. Zakharov v. Venäjä, 4.12.2015). Euroopan unionin oikeuden soveltamisalalla käsitteitä yleinen tai kansallinen turvallisuus tulee tulkita unionin oikeuden ja näitä käsitteitä tämentävän Euroopan unionin tuomioistuimen oikeuskäytännön valossa. EU-tuomioistuin lähtee vakiintuneesti siitä, etteivät jäsenvaltiot voi kukin yksinään ilman unionin toimielinten valvontaa määritellä unionin oikeuden soveltamiseen liittyen sellaisten käsitteiden kuin yleinen tai kansallinen turvallisuus ulottuvuuksia (Ks. esim. tuomio J.N., C-601/15, 65—66 kohta.). (HE 198/2017 vp, s. 35)

Kansallisen turvallisuuden alaan kuuluvat toiminnot määritellään toimivaltuuksien käytön näkökulmasta tyhjentävästi poliisilain 5 a luvun 3 §:ssä ja sitä vastaavalla tavalla tietoliikennetiedustelulain 3 §:ssä. Lakiehdotuksissa käytetty uhkaperusteinen määrittelytapa ja laissa mainitut uhkat ovat sopusoinnussa EIT:n ratkaisukäytännön kanssa. EIT:n ratkaisusta Zakharov v. Venäjä (2015) voidaan päätellä (erit. ratkaisun kohdat 247–248), että tällainen kansallisen turvallisuuden käsitteellisen määrittelytapa on ihmisoikeussopimuksen näkökulmasta suotava.

10 Tiedustelumenetelmien käyttöalan laajentuminen suhteessa nykyisiin rikostorjuntatoimivaltuuksiin

Eduskunnan oikeusasiamies kiinnittää huomiota seuraaviin seikkoihin:

a) Kun kohteena on henkilö (6 §), tiedusteluviranomainen voi kohdentaa telekuuntelua uusiin laitteisiin ja liittymiin, joiden oletetaan olevan henkilön käytössä. Tällaisessa menettelyssä teleosoitteen ja telepäätelaitteen liityntä tiedonhankinnan kohteena olevaan henkilöön jää tuomioistuinkontrollin ulkopuolelle.

Sisäministeriön vastaus: Tämä ei vaikuta alentavasti tiedusteluviranomaisen näyttötaakkaan sen suhteen, että teleosoitteella tai telepäätelaitteella on riittävä liityntä tiedonhankinnan kohteena olevaan henkilöön. Laitteen tai osoitteen sekä henkilön välinen liityntä tulee jokaisessa tapauksessa pystyä perustelemaan riittävällä tavalla.

Teleosoitteen tai telepäätelaitteen liityntä tiedonhankinnan kohteena olevaan henkilöön on tiedusteluvaltuutetun suorittaman reaaliaikaisen ja jälkikäteisen laillisuusvalvonnan kohteena. Nykyisin tällainen valvontajärjestelmä puuttuu kokonaan.

b) Tiedustelussa monien keinojen kohteena voi olla henkilöryhmä, kun taas salaisessa tiedonhankinnassa samojen keinojen kohteena on oltava henkilö.

Sisäministeriön vastaus: Mahdollisuus kohdistaa tiedustelumenetelmä ryhmään henkilön sijasta liittyy vain tiettyihin tiedustelumenetelmiin, eli suunnitelmalliseen tarkkailuun, peiteltyyn tiedonhankintaan, tekniseen kuunteluun, tekniseen katseluun ja peitet toimintaan. Kyseiset menetelmät ovat tyypillisesti sellaisia, että tiedonhankinnan kohteena ei ole yksilö vaan ryhmä henkilöitä taikka paikka, jossa kyseinen ryhmä oleskelee. Mahdollisuutta kohdistaa tiedonhankintaa ryhmään ei siten ole kaavailtu liitettäväksi esimerkiksi televalvontaan tai telekuunteluun.

Hallituksen esityksessä tarvetta kohdistaa tiedonhankintaa ryhmään yksilön sijasta perustellaan sillä, että tiedustelussa käytettävien toimivaltuuksien käytön tarkoituksena voi olla esimerkiksi tiedonhankinta henkilöryhmän organisaatiosta, ryhmään kuuluvista henkilöistä ja henkilöryhmän aktiivisuudesta tietyillä alueilla sekä ryhmän toiminnan eri muodoista.

Tiedustelussa kohdehenkilölle tehtävällä ilmoituksella ei tosiasiaa ole yhtä keskeistä merkitystä keinon käytön jälkikäteiskontrollissa kuin sillä on perinteisten salaisten tiedonhankintakeinojen ja salaisten pakkokeinojen järjestelmässä. Nykyisestä sääntelystä poiketen henkilöllä olisi mahdollisuus tehdä tiedustelumenetelmän käytön lainmukaisuutta koskeva tutkimispyyntö tiedusteluvaltuutetulle siihen katsomatta, onko hän tullut tietoiseksi itseensä kohdistuneesta tiedustelusta ilmoituksen johdosta. Tätä vasten on syytä huomata, että useat nyt puheena olevista menetelmistä (suunnitelmallinen tarkkailu, peitelty tiedonhankinta, peitet toiminta) ovat sellaisia, että niistä ei nykyisinkään ole velvollisuutta ilmoittaa kohdehenkilölle, jos asiassa ei ole aloitettu esitutkintaa (Poll 5 luvun 58 §:n 5 mom), mutta vastaavaa tutkimispyyntöä ei ole mahdollista tehdä.

Hallituksen esityksessä henkilöryhmää käsitellään suunnitelmallista tarkkailua koskevan 5a luvun 9 §:n yksityiskohtaisissa perusteluissa (HE 202/2017 vp., s. 185–186): ”Ollakseen henkilöryhmä tulisi siihen kuulua vähintään kolme henkilöä. Kyseisten henkilöiden tulisi muodostaa tietyn ajan koossa pysyvä ja rakenteeltaan jäsentynyt yhteenliittymä, joka toimii yhteistuumin tai heillä on ainakin yhteinen tavoite, kuten esimerkiksi vakavan pelon aiheuttaminen väestön keskuudessa tai tiedon hankkiminen Suomen ulko- ja turvallisuuspoliittisesta päätöksenteosta. Henkilöryhmän toiminnassa kysymys on eräänlaisesta organisaatiokulttuurista, jota saattaa ilmentää havaittavissa olevat näkyvät rakenteet, kuten käskyvaltasuhteet henkilöryhmän jäsenten välillä, tietyt arvot ja normit sekä perusoletukset, kuten käsitykset ja uskomukset. Kuuluakseen henkilöryhmään tulee yksittäisen henkilön toimia henkilöryhmän tavoitteiden mukaisesti tai ainakin edesauttaa niiden saavuttamista olennaisella tavalla. Henkilöryhmän voisi muodostaa esimerkiksi tietyn ulkomaisen tiedustelupalvelun tiedustelu-upseerit.

Vähimmän haitan periaatteen mukaisesti tulee toimivaltuuden käyttö ensisijaisesti kohdistaa tiettyyn henkilöön. Tiedustelutoiminnassa saattaa kuitenkin olla tarpeen selvittää keitä johonkin tiettyyn henkilöryhmään kuuluu tai voi olla tarpeen selvittää tietyn ryhmän esimerkiksi terroristiryhmän tai vieraan tiedustelupalvelun organisaation henkilöiden toimintaa tietyllä alueella. Silloin, kun tiedonhankinta kohdistuisi johonkin tiettyyn henkilöryhmään eikä se täsmentyisi Suomessa olevaan yksittäiseen tai yksittäisiin henkilöihin, niin 46 §:ssä tarkoitettua ilmoitusta ei olisi tarpeen tehdä. Jos tiedustelumenetelmän käyttö kohdistuisi johonkin tiettyyn Suomessa olevaan henkilöryhmään ja ryhmästä yksilöityisi henkilö niin, että hänen henkilöllisyytensä selviäisi, niin tiedustelumenetelmän käytöstä ilmoittamiseen sovellettaisiin tiedustelumenetelmän käytöstä ilmoittamista koskevaa 46 §:ää samalla tavoin kuin suunnitelmallinen tarkkailu olisi kohdistettu henkilöön.”

c) Tiedustelussa telekuunteluun voidaan käyttää tiedusteluviranomaisen omia laitteita, kun taas salaisessa tiedonhankinnassa käytetään säännönmukaisesti ulkopuolista operaattoria.

Sisäministeriön vastaus: Edellä sanotusta poiketen telekuuntelua koskeva poliisilain 5 luvun 5 §:n ja pakkokeinolain 10 luvun 3 §:n sääntely ei nykyisinkään sisällä vaatimusta, jonka mukaan telekuuntelu saadaan toteuttaa ainoastaan teleoperaattorin avustuksella. Laki on tältä osin toteuttamistapaneutraali.

Teleoperaattori ei myöskään ole toiminnan laillisuutta valvova taho. Operaattorin mahdollista mukanaoloa merkittävämpänä oikeusturvatakeena voitaneen pitää sitä, että telekuuntelun käyttöä tiedustelumenetelmänä valvoo paitsi ennakkollisesti tuomioistuimien, myös reaaliaikaisesti ja jälkikäteisesti tiedusteluvaltuutettu. Poliisilain 5 a luvun 61 §:n 1 momentti velvoittaisi suojelupoliisin ilmoittamaan mahdollisimman pian jokaisesta telekuuntelua koskevasta päätöksestä tiedusteluvaltuutetulle, joka valvoisi päätöksen täytäntöönpanon lainmukaisuutta. Nykyisestä sääntelystä tällainen oikeusturvamekanismi puuttuu täysin.

Tiedusteluvaltuutetulla tulee olemaan oikeus salassapitosäännösten estämättä saada suojelupoliisilta kaikki valvontatehtäviensä hoitamiseksi tarvitsemansa tiedot. Näin ollen tiedusteluvaltuutetulla on oikeus saada tiedot myös suojelupoliisin käyttämistä laitteista kuten myös miten ja missä niitä käytetään. Tässä yhteydessä olennaista on se, että muulla tapaa kuin operaattorin välityksellä toteutettava telekuuntelu edellytetään dokumentoitavan kattavasti lokituksen avulla tiedusteluvaltuutettua varten.

d) Salaisessa tiedonhankinnassa teleosoitteen ja telepäätelaitteen yksilöintitietojen hankintaan käytettävä laite ei saa mahdollistaa telekuuntelua, kun taas tiedustelussa tällaista rajoitusta ei ole. (15 §)

Sisäministeriön vastaus: Poliisilain olemassa olevan 5 luvun 25 §:n 2 momentin mukaan poliisi saa käyttää teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimiseksi ainoastaan sellaista teknistä laitetta, jota voidaan käyttää vain teleosoitteen ja telepäätelaitteen yksilöimiseen. Säännös merkitsee ainoastaan sitä, ettei sitä nimenomaista laitetta, jonka avulla yksilöintitiedot hankitaan, saa käyttää sen ohella telekuunteluun. Säännös ei siis nykyisinkään estä sitä, että telekuuntelu suoritetaan vastaavanlaisen laitteen avulla. Käytännössä nykyisestä sääntelyratkaisusta ainoastaan seuraa, että poliisilla on oltava kaksi samankaltaista laitetta mukanaan - yksi, jota voidaan käyttää ainoastaan yksilöintitietojen hankkimiseen ja toinen, jota voidaan käyttää ainoastaan telekuunteluun. Nykyinen sääntelyratkaisu olisi erittäin kallis ja erityisesti (ulkomaan) tiedustelua ajatellen on vaikea hahmottaa sellaisen sääntelyratkaisun ratiota.

e) Salaisessa tiedonhankinnassa tietolähteenä olevalle yksityiselle henkilölle ei voida luoda vääriä henkilö- ym. tietoja missään olosuhteissa, kun taas tiedustelussa se on mahdollista tietolähteen turvaamiseksi.

Sisäministeriön vastaus: Ks. edellä kohta 5.1.

f) Salaisen tiedonhankinnan keinoja voidaan Suomen viranomaisen päätöksin käyttää vain Suomessa, kun taas tiedustelussa samoja keinoja voidaan käyttää myös ulkomailla suojelupoliisin päällikön päätöksellä. Lakiehdotuksessa tai sen perusteluissa ei ole lainkaan käsitelty sitä tilannetta, että tiedustelumenetelmiä kohdennetaan Suomen ulkopuolella olevaan suomalaiseen. En pidä mahdollisena, että Suomen ulkopuolella vaikkapa lomalla olevaan suomalaiseen kohdennettaisiin suomalaisen tiedusteluviranomaisen toimesta esimerkiksi telekuuntelua ilman samaa päätöksentekomenettelyä ja oikeusturvatakeita kuin Suomessa olisi sovellettava. Nykyisin salaisessa tiedonhankinnassa ulkomailla olevan suomalaisen telekuuntelu edellyttää suomalaisen tuomioistuimen lupaa ja toiselle valtiolle osoitettua oikeusapupyyntöä ja kohdemaassa oikeusapupyynnön täytäntöönpanoa kyseisen valtion lainsäädännön mukaisesti.

Sisäministeriön vastaus: Siviilitiedustelua ja sotilastiedustelua koskevien hallitusten esitysten kansainvälisestä vertailusta voidaan havaita, että ulkomailla tehtävää tiedonhankintaa koskeva päätöksenteko vaihtelee maittain. Päätöksenteosta voi vastata esimerkiksi tiedusteluviranomainen itse tai jokin poliittisesti vastuunalainen taho. Jos päätöksenteosta vastaa tiedusteluviranomainen, tapahtuu se yleensä valtiojohdon linjausten puitteissa. Myös käsiteltävänä olevissa esityksissä ehdotetaan, että tiedusteluviranomainen päättää ulkomaan tiedustelusta, mutta se tapahtuu valtiojohdon linjausten mukaisesti.

Tiedustelussa käytettävät menetelmät kohdistuvat vieraan valtion suvereniteettiin kohdemaassa ja myös mahdollisesti kolmannessa valtiossa, jonka kautta tiedonhankintaa tehdään. Tämän vuoksi ulkomaan tiedustelun poliittinen ulottuvuus korostuu. Tiedustelun mahdolliset vaikutukset ja riskit vaikuttaisivat päätöksentekomenettelyyn. Ulkomailla tehtävästä siviilitiedustelusta ja tiedustelumenetelmän käytöstä päättäisi aina suojelupoliisin päällikkö. Suomalaisilla tuomioistuimilla ei ole toimivaltaa päättää menetelmien käytöstä Suomen alueen ulkopuolella eikä se tästä syystä tule kyseeseen päätöksentekotahona. Lisäksi ulkomaantiedustelun ulkopoliittisten herkkyyksien vuoksi on perusteltua, että riskin menetelmien käyttämisestä kantaisi ulkomaantiedustelua suorittava taho eli suojelupoliisi.

Tiedustelumenetelmien käytössä yleisenä edellytyksenä siviilitiedustelussa on, että sillä voidaan perustellusti olettaa saatavan tietoja sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Tarkoituksena ei ole eritellä kohdistuuko vakava uhka Suomen kansalliselle turvallisuudelle suomalaisen vai ulkomaalaisen henkilön toimesta. Ulkomaan tiedustelussa voidaan perustellusti kysymyksen 1) Kenelle Suomen tulisi tehdä kohdemaassa tehtävää salaista tiedonhankintaa koskeva oikeusapupyyntö? Ulkomaan tiedustelussa on lähtökohtaisesti välttämätöntä suorittaa salaista tiedonhankintaa Suomen kansallisen turvallisuuden suojaamiseksi ja tiedon hankkimiseksi siviilitiedustelun kohteena olevasta toiminnasta, joka muodostaa vakavan uhkan Suomen kansalliselle turvallisuudelle. 2) Onko yleensä mahdollista asettaa ulkomaan tiedustelussa suomalaista erityisasemaan ja millä perusteella? Jos suomen kansalainen asetettaisiin tiedustelussa muihin kansalaisuuksiin nähden erityisasemaan, niin voidaan perustellusti kysyä asettaako tämä ihmiset eriarvoiseen asemaan kansalaisuuden perusteella. Kansalaisuuteen sidottu raja ei ole tarkoituksenmukainen ratkaisu, koska myös suomalainen voi osallistua

esimerkiksi sellaiseen toimintaan, joka muodostaa vakavan uhkan Suomen kansalliselle turvallisuudelle. Esitetylle rajaukselle ei ole perusteita tältä osin.

Sellaisessa tilanteessa, jossa suomalainen joutuisi tiedustelumenetelmän kohteeksi eikä tiedolla olisi merkitystä kansallisen turvallisuuden suojaamiseksi, tieto hävitettäisiin välittömästi tiedon luonteen käytyä ilmi. Esimerkiksi telekuuntelun osalta suomalaisen käyttämän teleosoitteen perusteella voidaan kohtuullisella vaivalla havaita, että kyseessä on suomalainen teleosoite. Lisäksi on syytä todeta, että henkilö, joka kokee tai epäilee joutuneensa tiedustelumenetelmien käytön kohteeksi, voi aina tehdä tutkimispyynnön tiedusteluvaltuutetulle, että hän ryhtyisi tarvittaviin toimenpiteisiin.

g) Kaikkien tiedonhankintakeinojen käyttö ei edes edellytä, että sen kohteena oleva henkilö itse on osallistumassa kansallista turvallisuutta vakavasti uhkaavaan toimintaan.

Sisäministeriön vastaus: Siviilitiedustelulla tarkoitetaan suojelupoliisin suorittamaa tiedonhankintaa ja tiedon hyödyntämistä kansallisen turvallisuuden suojaamiseksi, ylimmän valtiojohton päätöksenteon tukemiseksi ja muiden viranomaisten lakisääteisiä kansalliseen turvallisuuteen liittyviä tehtäviä varten. Tarkoituksena ei ole hankkia tietoa yksittäisestä henkilöstä, jota on syytä epäillä rikoksesta tai olettaa tämän sellaiseen syyllistyvän.

h) Esityksen perusteella jää epäselväksi ja hahmottomattomaksi, millä perusteella aloitetaan jokin tiedustelutehtävä, johon ehdotettuja tiedustelumenetelmiä käytetään. Ehdotetusta laista puuttuu sotilastiedustelua koskevaan ehdotukseen sisältyvän 9 §:n 6 kohdan kaltainen määritelmä tiedustelutehtävästä.

Sisäministeriön vastaus: Poliisilain 1 luvun 1 §:ää ehdotetaan muutettavaksi niin, että siihen lisätään (suoja)poliisin tehtäväksi kansallisen turvallisuuden suojaaminen. Edelleen poliisin hallinnosta annetun lain 10 §:n, jossa säädetään suojelupoliisin tehtävästä, 1 ja 2 momenttia ehdotetaan muutettavaksi. Pykäläehdotus olisi seuraavanlainen:

10 §

Suojelupoliisi

Suojelupoliisin tehtävänä on sisäministeriön ohjauksen mukaisesti hankkia tietoa kansallisen turvallisuuden suojaamiseksi sekä havaita, estää ja paljastaa sellaisia toimintoja, hankkeita ja rikoksia, jotka voivat uhata valtio- ja yhteiskuntajärjestystä tai valtakunnan sisäistä tai ulkoista turvallisuutta. Sen tulee myös ylläpitää ja kehittää yleistä valmiutta yhteiskunnan turvallisuutta uhkaavan toiminnan havaitsemiseksi ja estämiseksi.

Sisäministeriö määrää Poliisihallitusta kuultuaan tarvittaessa tarkemmin suojelupoliisin ja muiden poliisiyksiköiden välisestä yhteistoiminnasta ja yhteistyöstä.

Voimassa olevassa sisäministeriön määräyksessä (SMDno-2015-2080) täsmennetään suojelupoliisin tehtäviä. Kyseistä määräystä tarkistetaan ehdotettujen lakien tultua voimaan. Nykyisin suojelupoliisi tekee sisäministeriölle vuosittain ehdotuksen tiedonhankintaprioriteeteiksi sekä tarvittaessa ehdotuksen prioriteettien muuttamiseksi. Sisäministeriö asettaa vuosittain suojelupoliisin tiedonhankintaprioriteetit (HE 346/2014 vp s. 15). Asettamalla kyseiset prioriteetit sisäministeriö ohjaa suojelupoliisin toimintaa suuntaamalla sen tiedonhankintaa. Suojelupoliisin tiedonhankintaprioriteettien asettamista edeltää niiden valmisteleva käsittely ulko- ja turvallisuuspoliittisessa ministerivaliokunnassa. Kyse onkin kokonaisuutena arvioituna valtioneuvostotason ohjaus- ja yhteensovittamismekanismista. Tästä mekanismista ei ole annettu laintasoisia säännöksiä. Hyvin toimineesta ohjausmekanismista ei ole katsottu tarpeelliseksi jatkossakaan säätää laintasolla.

Sisäministeri kantaa poliittista vastuuta suojelupoliisin toiminnasta ja siksi hänen tulee olla tietoinen viraston toimialaan kuuluvista keskeisistä asioista. Tämän vuoksi suojelupoliisin on ilmoitettava tehtäviinsä kuuluvista yhteiskunnallisesti merkittävistä asioista sisäministerille sekä, silloin kuin niillä on merkittävää vaikutusta muuhun poliisitoimeen, myös poliisiylijohtajalle. Suojelupoliisin päällikön on lisäksi pidettävä sisäministeriö, tarkemmin sanoen sisäministeri, kansliapäällikkö ja poliisiosaston ylijohtaja, tietoisena suojelupoliisia koskevista asioista (HE 346/2014 vp, s. 15). Suojelupoliisi informoi myös tasavallan presidenttiä, pääministeriä ja ulkoasiainministeriä sekä eduskunnan perustuslaki-, hallinto- ja ulkoasiainvaliokuntia pitääkseen heidät ajan tasalla ulko- ja turvallisuuspolitiikkaan liittyvistä asioista ja turvallisuustilanteesta (HE 58/2009 vp, s. 19).

11 Tietoliikennetiedustelun yleisen, kohdentamattoman ja kaiken kattavan seurannan kieltö

Eduskunnan oikeusasiamies katsoo, että tiedonhankinnan kohdentamisen epätasällisuus korostuu erityisesti tietoliikennetiedustelussa, jossa on kysymys tietoliikenteen automatisoituun erotteluun perustuvasta teknisestä tiedonhankinnasta. **VTT** käsittelee liikenne kysymystä massavalvonnasta. Ollakseen tehokas, lainsäädäntö edellyttää, että jokaiseen rajat ylittävään pisteeseen luodaan edellytykset tietoliikennetiedustelulle. **Professori Olli Mäenpää** toteaa lausunnossaan, että lakiin olisi yksityiskohtaisten lupaedellytysten lisäksi ja niiden soveltamista ohjaamaan perusteltua lisätä riittävän täsmällisesti määritelty yleissäännös, joka sisältäisi kiellon toteuttaa massavalvontaa. Tällainen yleiskielto olisi omiaan selventämään nyt vain esityksen perusteluissa mainittuja tietoliikennetiedustelun rajoja. Lisäksi se konkretisoisi Euroopan ihmisoikeussopimukseen ja EU:n perusoikeuskirjaan perustuvia luottamuksellisen viestin suojan perusvaatimuksia viranomaistoiminnassa merkityksellisellä tavalla. **Professori Tuomas Ojanen** toimittamassaan lausunnossa esittämän näkemyksen mukaan olisi kuitenkin syytä säätää tietoliikenteen yleisen, kohdentamattoman ja kaiken kattavan seurannan kiellosta tiedustelutoiminnassa nimenomaisesti sotilastiedustelu- ja siviilitiedustelulaeissa siltä osin kuin niissä säädetään tiedonhankinnasta tietoliikenteestä. Tämä loisi osaltaan takeita niiden sääntelyn sopusoinnulle EU-oikeuden (samoin kuin Euroopan ihmisoikeussopimuksen) kanssa. (En ota tässä vaiheessa yksityiskohtaisemmin kantaa kieltoäännöksen muotoiluun, vaan tyydyn painottamaan tarvetta tällaiselle kieltoäännökselle Euroopan ihmisoikeussopimuksen ja EU-oikeuden kannalta.) **VTT, BaseN ja CSC** toteavat, että tiedusteluviranomaisille luotaisiin teknisten edellytykset valvoa kaikkea tietoliikennettä kaikissa tietoliikenteen solmukohdissa. Lisäksi lausunnoissa todetaan, että myös Suomen sisäinen liikenne saattaa joutua tietoliikennetiedustelun piiriin. **Google** ilmaisee huolen siitä, että lainkohdat sellaisena kuin ne nyt on ilmaistu, voitaisiin tulkita laajentavasti siten, että tulkinta mahdollistaisi tietojen massakeräämisen ja -tiedustelun. **Amnesty international** katsoo, että viestintään kohdistuva tiedustelu voi olla ihmisoikeusnäkökulmasta hyväksyttävää tiettyjen tiukkojen edellytysten täyttyessä. Amnesty vastustaa viestinnän laajalle ulottuvaa ja massamittaista tarkkailua, kaappaamista, keräämistä, varastointia tai analysointia, jota ei ole kohdistettu tiettyyn yksilöön, ryhmittymään tai sijaintiin ja joka ei pohjaudu perusteltuun epäilyyn. Tällainen kohdentamaton ”massavalvonta” loukkaa suhteettomasti yksilön yksityisyyden suojaa ja sananvapautta, eikä voi olla hyväksyttävissä perus- ja ihmisoikeuksien valossa.

Sisäministeriön vastaus: Sisäministeriö katsoo, että tietoliikennetiedustelu ei muutu massavalvonaksi valmiuksia rakentamalla, vaan olennaista on toimivaltuuden käyttäminen tiedustelutoimintaan. Niiden kannalta asiaan vaikuttavia olennaisia tekijöitä ovat käyttötarve, tosiasialliset resurssitekniset edellytykset sekä viranomaisen toimivaltuudet. Suomen sääntelymalli eroaa verrokkivaltioista olennaisesti siinä, että Suomessa viestin sisältöön kohdistuvat haku ehdot eivät ole mahdollisia. Tällöin tiedustelun tekninen toteuttaja ei voi irrottaa tietoliikennevirrasta satunnaista datamassaa sisältöhakuehtovertailuun, vaan irrotettava aineisto on ensin valikoitava teknisten hakuehtojen perusteella.

Suomen perustuslain 10 §:n muuttamista koskevassa hallituksen esityksen yksityiskohtaisissa perusteluissa todetaan, että: ”[Perustuslain] Säännöksessä mainittavasta ja perusoikeuksien yleisiin rajoitusedellytyksiinkin kuuluvasta välttämättömyysvaatimuksesta ja vaatimuksesta rajoituksen sopusoinnusta kansainvälisten ihmisoikeusvelvoitteiden kanssa samoin kuin EU-oikeudesta seuraa vaatimuksia muun muassa toimivaltuuksien yksilöimiselle. Ehdotettu sääntely ei siten mahdollistaisi yleisestä, kohdentamattomasta ja kaikenkattavasta tietoliikenteen seurannasta säätämistä.”

Kyseinen asia mainitaan myös siviilitiedustelua koskevassa hallituksen esityksessä (HE 202/2017 vp., s. 272): ”Selvää joka tapauksessa on, että perustuslain 10 §:n 3 momentin nojalla ei ole mahdollista säätää sellaisista rajoituksista viestin salaisuuteen, joiden tarkoituksena ei olisi yksilöidyn rikoksen torjuminen, vaan laajemmalti kansallisen turvallisuuden kannalta välttämättömän tiedon hankkiminen vakavista uhkista. Näin ollen telekuuntelun ja sen sijasta tehtävän tietojen hankkimisen, televalvonnan, teknisen kuuntelun, lähetyksen jäljentämisen ja tietoliikennetiedustelun menetelmin tehtävästä tiedonhankinnasta kansallisen turvallisuuden suojaamiseksi olisi mahdollista säätää tavallisen lain säätämisjärjestyksessä vain perustuslain 10 §:n 4 momenttiin ehdotetun tiedon hankkimista koskevan uuden rajoitusperusteen nojalla ja edellyttäen, että sääntely täyttää perusoikeuksien yleiset rajoitusedellytykset. Perustuslain 10 §:n 4 momenttiin ehdotetun tiedon hankkimista koskeva uusi rajoitusperuste ei mahdollista yleisestä, kohdentamattomasta ja kaiken kattavasta tietoliikenteen seurannasta säätämistä.”

Sisäministeriö pitää edellä mainittuja rajauksia riittävänä eikä katso tarkoituksenmukaiseksi säätää nimenomaisesta tietoliikenteen yleisen, kohdentamattoman ja kaiken kattavan seurannan kiellosta laissa tietoliikennetiedustelusta siviilitiedustelussa.

Osana tietoliikennetiedustelun toteuttamista kartoitetaan se viestintäverkon osa eli ne yhteydet, joissa kulkee siviilitiedustelun kannalta merkityksellinen liikenne. Kyseiset yhteydet voivat vaihdella ja muutoksiin reagoidaan. Tiedustelutoiminnassa ei ole tarkoituksenmukaista eikä edes tarvetta rakentaa jatkuvaa ja kaiken kattavaa seurantaa kaikkiin tietoliikenneyhteyksiin tai tietoliikenteen solmukohtiin. Suojelupoliisin sekä sotilastiedusteluviranomaisella on ennen teknisen kytkennän tekemistä viestintäverkon osaan pääsääntöisesti sellaista ennakkotietoa, jottei liityntäpisteiden rakentaminen ei tapahdu sattumanvaraisesti.

Tietoliikennetiedustelu ei olisi mahdollista, ellei tiedustelua voitaisi kohdistaa niihin tietoliikenneyhteyksiin, joissa kulkee tiedustelun kannalta merkittävää tietoliikennettä. Tämä ei kuitenkaan tarkoita sitä, että kyseisen tietoliikenneyhteyden kaikkea tietoliikennettä seurattaisiin. Jotta tietoliikennetiedustelua voitaisiin käyttää, tarvitaan aina tuomioistuimen lupa, jossa olisi ilmoitettava 1) tietoliikennetiedustelun kohteena oleva toiminta [siviilitiedustelun kohteet], 2) kyseistä toimintaa koskevat tosiseikat, 3) tosiseikat, joihin tietoliikennetiedustelun käytön edellytykset perustuvat⁵, 4) tietoliikennetiedustelussa käytettävät hakuehdot tai hakuehtojen luokat sekä perustelut niille, 5) rajan ylittävän viestintäverkon osa, jossa liikkuvaan tietoliikenteeseen hakuehtoja käytetään, sekä perustelut viestintäverkon osan valinnalle, 6) tietoliikennetiedustelua koskevan luvan voimassaoloaika kellonajan tarkkuudella, 7) tietoliikennetiedustelun suorittamista johtava ja valvova tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystään kuuluva poliisimies, 8) mahdolliset tietoliikennetiedustelun rajoitukset ja ehdot⁶.

Jos tuomioistuin myöntää luvan tiedusteluviranomaiselle, tietoliikennetiedustelun käytön aloittaminen edellyttää ulkopuolisen kytkennän suorittajan suorittamaa kytkentää tuomioistuimen myöntämän luvan tarkoittamaan viestintäverkon osaan. Myös tämä takaa sen, ettei tiedusteluviranomaisella ole suoraa pääsyä kaikkeen tietoliikenteeseen.

Tietoliikennetiedustelulaissa ehdotetaan säädettäväksi myös tiedustelukielloista (20 §). Tietoliikennetiedustelua ei saa kohdistaa viestiin, jonka lähettäjä ja vastaanottaja ovat Suomessa, eikä tietoon, josta lähettäjällä tai vastaanottajalla taikka tallentajalla on velvollisuus tai oikeus kieltäytyä todistamasta oikeudenkäymiskaaren 17 luvun 13, 14, 16 tai 20 §:n taikka 22 §:n 2 momentin nojalla. Tietoliikennetiedustelulla saatu tieto on hävitettävä viipymättä, jos käy ilmi, että se on kohdistunut tiedustelukiellon alaiseen tietoon. Käytännössä tämä tapahtuu pääosin tietoliikenteen käsittelyn automatisoidun käsittelyn vaiheessa. Jos tiedustelukiellon alaista tietoa päättyy manuaalisen käsittelyn vaiheeseen, sitoo hetihävittämisvelvollisuus edelleen tietoliikennettä käsittelevää virkamiestä.

Lopuksi on syytä todeta, että siviilitiedustelulainsäädäntö mahdollistaa tiedustelutoimivaltuuksien käytön defensiivisesti. Tämä tarkoittaa sitä, että tietoliikennetiedustelua ja muita tiedustelumenetelmiä tiedusteluviranomainen saa käyttää ainoastaan, jos pitää hankkia tietoa sellaisesta laissa tyhjentävästi säädetyistä toiminnasta [siviilitiedustelun kohteet], joka muodostaa vakavan uhkan Suomen kansalliselle turvallisuudelle. Näin ollen tietoliikenneyhteyksien seuraaminen valvonnallisessa merkityksessä ei ole tiukkojen sekä täsmällisesti ja tarkkarajaisesti määriteltyjen oikeudellisten edellytysten perusteella mahdollista.

BaseN Oy kiinnittää huomiota viestintäverkoissa liikkuvan tietoliikenteen määrään. Lisäksi lausunnossa kiinnitetään huomiota tietoliikenteen salaukseen.

Sisäministeriön vastaus: Kaapeleiden ja kuitujen osalta on huomioita se, että niistä mainitaan käytännössä aina niiden kokonaiskapasiteetti, mikä ei käytännössä koskaan ole käytössä. Lisäksi kaikkia Suomen rajan ylittävät kaapelit ja kuidut eivät ole käytössä kaiken aikaa.

⁵ 4 §. Tietoliikennetiedustelun käytön edellytykset.

Tietoliikennetiedustelun käytön yleisenä edellytyksenä on, että sillä voidaan perustellusti olettaa saatavan tietoja sellaisesta tietoliikennetiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Jos tietoliikennetiedustelun hakuehtojen käyttö ei koske ainoastaan valtiollisen toimijan tai siihen rinnastuvan tahon tietoliikennettä, on edellytyksenä lisäksi, että tietoliikennetiedustelun voidaan olettaa olevan välttämätöntä tiedon saamiseksi tietoliikennetiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

⁶ Tuomioistuin voi asettaa tietoliikennetiedustelun käytölle rajoituksia ja ehtoja. Myös tiedusteluviranomainen voi oma-aloitteisesti esittää hakemuksessa tietoliikennetiedustelun käytölle rajoituksia ja ehtoja.

Tietoliikennetiedustelussa pystytään valitsemaan merkitykselliset viestintäverkkojen osat ja suodattamaan pois epäoleellista liikennettä.

Julkisista lähteistä saatujen tietojen mukaan noin puolet tietoliikenteestä on tällä hetkellä salattua. Tietoliikennetiedustelulla voidaan salauksesta huolimatta saada kansallisen turvallisuuden kannalta merkittävää tietoa esimerkiksi tunnistamistietojen perusteella. Tietoliikennetiedustelua käytettäisiin myös tietoverkkohyökkäysten havaitsemiseen, johon mahdollisella salaamisella ei ole vaikutusta. Tämän lisäksi myös salatusta tietoliikenteestä voidaan muodostaa olennaista tiedustelutietoa salausta purkamatta. Tietoliikennetiedustelujärjestelmän riittävä tehokkuus voidaan varmistaa vaatimatta yrityksiltä salausavaimia tai takaporttien asentamista.

Tietoliikennetiedustelun tehokkuus on kyseenalaistettu myös sen perusteella, että tietoliikennemäärät kasvavat tulevaisuudessa. Tietoliikennemäärien kasvun ei kuitenkaan voida katsoa vähentävän tietoliikennetiedustelun tarpeellisuutta, vaan pikemminkin lisäävän sitä. Tietoliikennemäärien kasvuun on voitava vastata toiminnan riittävällä resursoinnilla ja huolehtimalla siitä, että tiedusteluprosessi on riittävän valikoiva.

Suomen internet-yhdistys SIY ry katsoo lausunnossaan, että massavalvonnan välttäminen olisi toteutettavissa parhaiten vaihtamalla tietoliikennetiedustelua koskevan lakiehdotuksen terminologiaa niin, että viestintäverkon osa vaihdettaisiin yhteysväliksi, jolloin tiedustelun toteutus rinnastuisi pakkokeinolakiin.

Sisäministeriön vastaus: Viestintäverkon käsite on suomalaisessa lainsäädännössä vakiintunut. Viestintäverkolla tarkoitetaan toisiinsa liitetystä johtimista sekä laitteista muodostuvaa järjestelmää, joka on tarkoitettu viestin siirtoon tai jakeluun johtimella, radioaalloilla, optisesti tai muulla sähkömagneettisella tavalla. Viestintäverkon osalla tarkoitaisi siis jotain sellaista osaa, josta tietoliikennetiedustelulla voitaisiin saada tiedustelutehtävän edellyttämä tieto tietystä tietoliikennevirrasta.

Viestintäverkon osa ja yhteysväli olisivat käytännössä synonyymejä, sillä tietoliikennetiedustelu kohdistuisi viestintäverkon osan kautta liikkuvaan tietoliikenne virtaan eli tietyssä yhteysvälissä liikkuvaan tietoliikennevirtaan.

Edellä kerrotun perusteella viestintäverkon osa on terminä tarkempi eikä terminologiaa tulisi tältä osin muuttaa.

12 Valtiollinen toimija

Eduskunnan oikeusasiamies kiinnittää huomiota siihen, ettei hallituksen esityksessä määritellä, millä todennäköisyydellä tiedustelun kohteena oleva tahon on oltava määriteltävissä valtiolliseksi toimijaksi.

Hallituksen esityksessä käsitellään valtiollista toimijaa mm. seuraavasti (HE 202/2017 vp., s. 179–180): ”Pykälän 3 momentissa säädettäisiin matalammasta käyttökynnyksestä niissä tapauksissa, joissa tiedustelumenetelmän käyttö kohdistetaan valtiolliseen toimijaan tai siihen rinnastuvaan tahoon. Luottamuksellisen viestin suojaan puuttuvan tiedustelumenetelmän kohdalla tämä tarkoittaisi, että esimerkiksi telekuuntelun käyttö pystyttäisiin kohdistamaan kahden valtiollisen toimijan väliseen viestintään, joka ei nauti perustuslaissa säädettyä luottamuksellisen viestin suojaa. Tällainen tilanne voisi olla esimerkiksi silloin, jos viestintä tapahtuu viranomaisverkossa. Mikäli virkamies käyttäisi viranomaisverkkoa yksityispuhelukensa soittamiseen, niin hän samalla ottaa riskin siitä, että viestinnän toinen osapuoli myös joutuu tiedustelun kohteeksi. Oletuksena on, että viranomaisverkkoja käytetään ainoastaan viranomaisten väliseen viestintään.

Viranomaiseen toimijaan rinnastuvalla taholla kattaisi tilanteet, joissa esimerkiksi valtiossa ei olisi viranomaiseksi tunnistettavaa tahoa, mutta joka hoitaisi valtion asioita, kuten viranomainen. Tahoa voitaisiin arvioida esimerkiksi sitä kautta, voisiko Suomi tai suomalainen viranomainen tehdä sopimuksen tällaisen tahon kanssa tai voisiko taho olla kansainvälisen järjestön toiminnassa mukana.

Viranomaiseen toimijaan rinnastuvalla taholla tarkoitettaisiin myös viranomaisen puolesta toimivaa tahoa eli ns. välillistä toimijaa, joka toimii puhtaasti valtiollisen toimijan lukuun. Kyseessä voisi siten olla yksityinen taho, kuten yritys, muu ryhmittymä tai jopa yksittäinen henkilö. Tällöin olennaista on arvioida esimerkiksi sitä, toimiiko tällainen taho valtion määräysvallassa tai sen ohjauksessa taikka

ottaako valtio tällaisen tahon toiminnasta vastuun itselleen. Esimerkiksi kaupalliseen yksityisoikeudelliseen sopimukseen perustuvia yrityksen velvollisuuksia valtiollista toimijaa kohtaan ei voida pitää sellaisena, minkä perusteella yritystä voitaisiin pitää valtiollisena toimijana. Huomiota olisi kiinnitettävä esimerkiksi siihen, minkälainen tosiasiallinen määräysvalta ja ohjaus valtiolla olisi yritykseen ja kuinka konkreettisesti valtio voisi määrätä yrityksen toiminnasta.

Muiden ryhmittymien osalta edellä sanotun lisäksi huomiota olisi kiinnitettävä siihen, kuinka järjestäytyneitä toiminta on, kuinka merkittävät resurssit ryhmittymällä on käytössään esimerkiksi aseellisen hyökkäyksen tekemiseksi ja voisiko tällainen hyökkäys tekona rinnastua vaikutuksiltaan vieraan valtion tekemäksi sekä pyrkiikö ryhmittymä toimimaan valtion tavoin.

Itsestään selvää olisi, että valtiollisen toimijan tulisi olla edeltä käsin tunnistettu valtiolliseksi toimijaksi ja toimijan valtiollinen asema olisi ilmeinen. Tämä tarkoittaisi sitä, että esimerkiksi tiedustelumenetelmän käytöstä päätettäessä tai lupavaatimusta laadittaessa suojelupoliisilla olisi ennakkotieto, että kohde olisi valtiollinen toimija ja tiedustelumenetelmän käytön aikana kohteena oleva toimisi tässä roolissa. Tiedustelutehtävän aikana tiedustelumenetelmän käyttö saattaisi alkaa muuhun kuin valtiolliseen toimijaan kohdistuvana tiedonhankintana, mutta tiedustelumenetelmällä saatujen tietojen perusteella tiedustelumenetelmän käyttö voisi myöhemmässä vaiheessa jatkaa valtiolliseen toimijaan kohdistuvana tiedustelumenetelmän käyttönä, jos kävisi ilmeiseksi kohteena olevan toimijan valtiollinen status. Viime kädessä päätöksentekijän olisi ratkaistava se, onko vaatimuksen tueksi esitetty riittävä tosiseikasto sen tueksi, että kohteena oleva taho olisi valtiolliseksi toimijaksi katsottava.”

Määritelmä itsessään jo osoittaa kohtuullisen korkeaa varmuuden astetta siitä, että tietty taho voidaan katsoa valtiolliseksi toimijaksi. Ratkaisua osaltaan puoltaa se, että lakiehdotuksessa valtiolliseen toimijaan kohdistettavien tiedustelumenetelmiä voitaisiin käyttää alemmin käyttöedellytyksin kuin muuhun tahoan, koska vieraan valtion sotilas- tai muun viranomaisorganisaation viestintä ei nauti luottamuksellisen viestin salaisuuden suojaa (PeVM 4/2018 vp., s. 7).

Valtiolliseen toimijaan liittyy aina tietty pysyvyys, eikä organisaatio muutu kovinkaan nopeatahtisesti. Valtio-organisaation voidaan olettaa toimivan aina suunnitelmallisesti jonkin tietyn tavoitteen toteuttamiseksi. Tavoitteet eivät muutu nopeatahtisesti vaikka tavoitteen saavuttamiseksi toteutettavat toimet ilmenisivätkin ulkopuolisille yllättäen.

Tiedustelumenetelmien käyttö voisi alkaa muuhun kuin valtiolliseen toimijaan kohdistuvana, ja tilanteen edetessä ja hankittujen tietojen pohjalta kohde voitaisiin tunnistaa valtiolliseksi toimijaksi. Näin myös valtiollinen toimija – asema olisi myös todennettavissa tarkemmin saatujen tietojen pohjalta.

13 Viranomaisyhteistyö ja tietojen luovuttaminen

Sisäministeriön rajavartio-osasto katsoo, että ylimmän valtiojohdon tiedonsaannin turvaaminen Suomen turvallisuusympäristön muutoksista ja kehitymisestä edellyttää, että suojelupoliisin hankkimaa tiedustelutietoa saatettaisiin perusteellisesti analysoituna myös muiden viranomaisten käyttöön.

Viestintävirasto katsoo viraston tehtävien hoitamisen kannalta olevan välttämätöntä, että suojelupoliisilla on salassapitosäännösten estämättä mahdollisuus luovuttaa tietoliikennetiedustelun avulla hankittu tieto haitallisesta tietokoneohjelmasta tai käskystä toimivaltaiselle viranomaiselle, kun tiedon luovuttaminen on tarpeen kansallisen turvallisuuden suojaamiseksi tai tiedon saajan etujen turvaamiseksi.

Helsingin poliisilaitos toteaa, että poliisi tarvitsee uhkien torjumiseksi tietojohtoisen poliisitoiminnan perustaksi ajantasaista, oikeaa ja riittävää tietoa käynnissä olevista uhkista, jotta se voi analysoidun tiedon avulla kohdistaa operatiivista toimintaansa ensisijassa ennalta ehkäisemään uhkat. Tärkeää on myös tiedostaa usean toimijan ympäristössä yhteistyön merkitys tiedon rikastamisessa ja siihen liittyen välttää tiedon sirpaloitumisen ja tiedonvälityksen viiveiden aiheuttamat aukot viranomaistoiminnassa, joita rikoksentekijät pyrkivät hyödyntämään.

Professori Olli Mäenpää toteaa, että yhteisöjen kanssa tehtävän yhteistyön sisältö on säännöksessä määritelty hyvin väljästi. Tarvetta tällaiselle yhteistyölle on käytännössä erityisesti erilaisten kyberuhkien torjunnassa. Perustelujen mukaan yhteistyö voisi liittyä myös yritysten turvallisuuteen ja yritysvakoilun estämiseen. Yhteistyöhön yhteisöjen kanssa sisältyisi myös oikeus luovuttaa tällaisille yhteisöille salassapitosäännösten estämättä tietoja, mikäli tietojen luovuttaminen on välttämätöntä

kansallisen turvallisuuden suojaamiseksi. Ehdotetun säännöksen mukaan salaisten tiedustelutietojen luovuttaminen yhteisöille olisi rajattu verraten väliin puitteisiin.

Sisäministeriön vastaus: Tietoliikennetiedustelusta siviilitiedustelussa ehdotetun lain 16 §:ssa esitetään säädettäväksi haitallista tietokoneohjelmaa tai -käskyä koskevien tietojen luovuttamisesta viranomaiselle, yritykselle tai yhteisölle. Pykälän 1 momentin mukaan: "Suojelupoliisi saa salassapitosäännösten estämättä luovuttaa tietoliikennetiedustelun avulla hankitun tiedon haitallisesta tietokoneohjelmasta tai käskystä viranomaiselle, yritykselle tai yhteisölle, jos tiedon luovuttaminen on tarpeen kansallisen turvallisuuden suojaamiseksi tai tiedon saajan etujen turvaamiseksi." Sisäministeriön näkemyksen mukaan kyseinen säännös turvaa Viestintäviraston tehtävien hoitamisen mainituilta osin.

Poliisilain muuttamista koskevan lakiehdotuksen 5 a luvun 55 §:ssä ehdotetaan säädettäväksi yhteistyöstä muiden viranomaisten ja yhteisöjen kanssa. Pykälän 2 momentin mukaan: "Suojelupoliisi voi siviilitiedustelutehtävänsä toteuttamiseksi toimia yhteistyössä yhteisöjen kanssa sekä luovuttaa muille viranomaisille ja yhteisöille salassapitosäännösten estämättä tietoja, jos tietojen luovuttaminen on *välttämätöntä* kansallisen turvallisuuden suojaamiseksi." Tietojen luovuttamisen kynnys on kyseisessä säännösehdoituksessa korkeampi kuin ensiksi mainituissa. Voidaan perustellusti kysyä onko "välttämättömyys" liian korkea kynnys tässä yhteydessä ja onko se yhdenmukainen tietoliikennetiedustelulakiehdotuksessa valitun kynnyksen "on tarpeen kansallisen turvallisuuden suojaamiseksi tai tiedon saajan etujen turvaamiseksi" kanssa.

Yleisemmässä luovuttamista koskevassa säännöksessä (PoL 5a:55.2) oleva kynnys "välttämätöntä" voi olla omiaan vaikeuttamaan ja supistamaan tiedusteluviranomaisen raportointitoimintaa ja yleisemminkin tiedon jakamista, koska yksittäisessä tiedonluovutustapauksessa tulisi pystyä erikseen osoittamaan, että tiedusteluraportin luovuttaminen on välttämätöntä kansallisen turvallisuuden suojaamiseksi. Koska siviilitiedustelulainsäädännön tarkoituksena on lisätä tiedusteluviranomaisen raportointia ja yhteydenpitoa muihin viranomaisiin sekä sitä kautta analysoidulla tiedustelutiedolla parantamaan kansallista turvallisuutta, niin sisäministeriö katsoo, että poliisilakiehdotuksen 5 a luvun 55 §:n 2 momentissa oleva kynnys muutettaisiin vastaamaan tietoliikennetiedustelulaissa käytettyä "jos tiedon luovuttaminen on tarpeen kansallisen turvallisuuden suojaamiseksi".

Teknologian tutkimusliitto VTT Oy (VTT) toteaa lausunnossaan, että tiedusteluviranomaisen tiedustelutarkoituksessa hyväkseen käyttämä tietojärjestelmän haavoittuvuus voisi olla myös tieto, joka saattaisi olla merkityksellinen yritysten suojaamisen kannalta. **Suomen puolustus- ja ilmailuteollisuusyhdistys PIA** katsoo, että olevan positiivista, että tiedustelun tuottamaa tietoa voitaisiin tarvittaessa luovuttaa yksityisille yhteisöille vakavien uhkien torjunnan mahdollistamiseksi tai merkittävien taloudellisten tappioiden estämiseksi.

Sisäministeriön vastaus: Siviilitiedustelun ensisijainen tavoite on Suomen kansallisen turvallisuuden parantaminen. Siviilitiedusteluviranomaisena toimivan suojelupoliisin tehtävänä tulee olemaan Suomen kansallisen turvallisuuden suojaaminen. Näin ollen myös mahdollista tietojärjestelmän haavoittuvuutta koskevaa tietoa ja sen luovuttamista arvioidaan Suomen kansallisen turvallisuuden suojaamisen näkökulmasta.

Mahdollista tietojärjestelmän haavoittuvuutta koskevan tiedon luovuttaminen yritykselle on aina tapauskohtaista harkintaa. Tietoliikennelakiehdotuksen 16 §:n 1 momentin mukaan suojelupoliisi saisi salassapitosäännösten estämättä luovuttaa tietoliikennetiedustelun avulla hankitun tiedon haitallisesta tietokoneohjelmasta tai käskystä viranomaiselle, yritykselle tai yhteisölle, jos tiedon luovuttaminen on tarpeen kansallisen turvallisuuden suojaamiseksi tai tiedon saajan etujen turvaamiseksi. Harkinnassa otetaan huomioon aina sekä Suomen kansallisen turvallisuuden suojaaminen että tiedon saajan edut. Voi olla, että kyseiset intressit ovat myös päällekkäisiä. Edellä tarkoitettujen tietojen luovuttamista koskevien kriteerien arvioinnissa sekä intressipunninnassa korostuu suojelupoliisin ammattitaito.

14 Teleyritysten kustannusten korvaaminen

FiCom, DNA, EK, Elisa Oyj, Telia Oyj ovat kiinnittäneet huomiota teleyrityksille maksettavien kulujen korvaamiseen. Ehdotetuista säännöksistä aiheutuisi teleyrityksille ja tiedonsiirtäjille kustannuksia, joiden määrä riippuisi poliisilain ehdotetun 5 a luvussa tarkoitettujen menetelmien sekä siviili- ja sotilastiedustelulaeissa tarkoitetun tiedustelun ja tiedonsiirtäjiltä vaadittavien toimenpiteiden kokonaismäärästä. Toimenpiteiden lukumäärä ei ole teleyritysten eikä tiedonsiirtäjien ennakoitavissa eikä myöskään kontrolloitavissa. Esityksen perusteella ei pysty ennakoimaan, tiedustelutoimenpiteistä teleyrityksille tai tiedonsiirtäjille aiheutuvia kustannuksia.

Sisäministeriön vastaus: Poliisilain muuttamista koskevan lakiehdotuksen 5 a luvun 52 §:ssä esitetään säädettäväksi korvauksesta teleyritykselle siviilitiedustelussa avustamisesta ja tietojen antamisesta. Korvauskäytäntö vastaisi sitä, mitä nykyisin poliisilain 5 luvussa 62 §:ssa ja pakkokeinolain 10 luvun 64 §:ssä osalta säädetään. Molempien lainkohtien mukaan teleyrityksellä on oikeus saada valtion varoista korvaus salaisten tiedonhankintakeinojen tai salaisten pakkokeinojen yhteydessä tapahtuvasta viranomaisen avustamisesta ja tietojen antamisesta aiheutuneista välittömistä kustannuksista siten kuin tietoyhteiskunta- ja sähköisen viestinnän palveluista annetun lain 299 §:ssä säädetään. Korvauskäytännöstä toisin sanoen säädetään sähköisen viestinnän palveluista annetun lain 299 §:ssä.

Korvauskäytännön muuttaminen kattamaan tältä osin kaikki kustannukset saattaisi aiheuttaa merkittäviä kustannusvaikutuksia erityisesti poliisille sekä myös muille esitutkintaviranomaisille, jotka käyttävät salaisia tiedonhankintakeinoja ja salaisia pakkokeinoja.

Siviilitiedustelua koskevan lainsäädäntökokonaisuuden yhteydessä puhtaasti yritystoiminnalle aiheutuvien euromäärien arvioiden osalta on syytä olla varovainen, koska niiden etukäteinen laatiminen voi johtaa helposti harhaanjohtavaan lopputulokseen. Esimerkiksi teletiedustelumenetelmien (telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta, tukiasematietojen hankkiminen) lukumäärät on ainoastaan hyvin yleispiirteisesti arvioitavissa ja ennakoitavissa.

Yleisellä tasolla voidaan kuitenkin arvioida, että lainsäädäntömuutoksen myötä teleyritysten työmäärä saattaisi lisääntyä, mutta työmäärän kasvua on omiaan hillitsemään tiedustelumenetelmiä koskevien lupa-aikojen pidentyminen. Tämä vähentäisi pidempikestoisessa tiedusteluoperaatiossa teleyrityksille aiheutuvaa henkilöresurssikuormitusta suhteessa siihen, kuin että luvat olisivat ajalliselta kestoaltaan yhden kuukauden mittaisia. Siviilitiedustelulainsäädäntöä koskevan esityksen taloudellisten vaikutusten arviointiin on sisällytetty euromääräisesti sanallinen kuvaus sekä yhteenvetotaulukot taloudellisista vaikutuksista koskien suojelupoliisia. Kyseisiin kuluihin on myös sisällytetty arvio yrityksille maksettavista korvauksista, joiden täsmällinen jaottelu ei tiedustelumenetelmiä koskevien lupamääräarvioiden takia ole julkista tietoa.

Sisäministeriön arvion mukaan teleyritysten vastuulle jäävät kustannukset olisivat marginaalisia. Tämä johtuu edellä kerrotun lisäksi siitä, että suojelupoliisin rooli muuttuu tiedustelullisempaan suuntaan eikä rikostorjuntatoimivaltuuksilla tulisi olemaan niin merkittävää roolia kuin aiemmin.

Kyse on kokonaan uudesta ja sellaisesta lainsäädäntökokonaisuudesta, että vaikutusten arvioinnissa korostuu etukäteisarvioinnin lisäksi erityisesti jälkikäteisarviointi. Siksi on perusteltua esittää eduskunnalle harkittavaksi, että se asettaa lainsäädännön täytäntöönpanon ja toteutumisen seurantavelvoitteen. Seurantajakson olisi tarkoituksenmukaista olla riittävän pitkä, jotta jälkikäteiseen arviointiin olisi saatavilla tarvittava määrä materiaalia. Seurannan mittareita asetettaessa olisi kuitenkin tärkeää, että ne muodostaisivat sellaisen kokonaisuuden, josta voidaan saada mahdollisimman laajaa ja objektiivista tietoa tarvittavien johtopäätösten tekemiseksi. Tiedustelutoimintaan liittyvät ulkopoliittiset ja muut sensitiivisyydet asettavat tiettyjä rajoitteita seurannan mittarien asettamisessa.

FICIX ry toteaa, että yhdysliikennepisteisiin kohdistettavilla tiedustelutoimenpiteillä ei saavuteta sille asetettuja tavoitteita.

Sisäministeriön vastaus: Sisäministeriö näkee FICIX ry:n lausuntoa vastaavasti, ettei yhdysliikennepisteisiin kohdistettavilla tiedustelutoimenpiteillä saavutettaisi tiedustelutoiminnan tavoitteita eikä yhdysliikennepisteitä nähdä merkittävänä siviilitiedustelun kannalta. Tämä ei kuitenkaan tarkoita sitä, etteivätkö yhdysliikennepisteet voisi olla tiedustelun kohteena, jos siviilitiedustelu olisi välttämätöntä kohdistaa yhdysliikennepisteeseen.

CSC esittää lausunnossaan, että yritysten henkilöstön oikeudellinen vastuu tulisi määritellä selkeästi silloin, kun yritys joutuisi avaamaan asiakkaiden luottamuksellista tietoliikennettä.

Sisäministeriön vastaus: Siviilitiedustelulainsäädäntö koskevassa hallituksen esityksessä ei esitetä säädettäväksi tai muutettavaksi sellaisia säännöksiä, joiden nojalla yritys voitaisiin velvoittaa avaamaan asiakkaansa luottamuksellista tietoliikennettä tiedusteluviranomaisen pyynnöstä.

Suomen Erillisverkot Oy toteaa, että kytkennän de-aktivoiminen tai purkaminen pitää vastaavalla tavalla perustua tuomioistuimen yksiselitteiseen päätökseen.

Sisäministeriön vastaus: Tietoliikennetiedustelulakiehdotuksen 7 §:n 2 momentin 6 kohdan mukaan tietoliikennetiedustelua koskevassa tuomioistuimelle osoitettavassa vaatimuksessa ja tuomioistuimen antamassa lupapäätöksessä on mainittava tietoliikennetiedustelua koskevan luvan voimassaoloaika kellonajan tarkkuudella. Näin ollen tuomioistuin käytännössä päättää myös kytkennän de-aktivoimisesta tai purkamisesta. On myös huomioitava, että poliisilain muuttamista koskevan lakiehdotuksen 5 a luvun 4 §:n 5 momentin mukaan tiedustelumenetelmän käyttö on lopetettava ennen päätöksessä mainitun määräajan päättymistä, jos käytön tarkoitus on saavutettu tai sen edellytyksiä ei enää ole. Kyseisellä säännöksellä korostetaan sitä, ettei tiedustelumenetelmiä voida missään tapauksessa käyttää kauempaa kuin on tarpeen, vaikka lupa olisikin vielä voimassa. Tämä ilmenee myös poliisioikeudellisista periaatteista, kuten vähimmän haitan periaatteesta, joiden merkitystä perustuslakivaliokunta on yleisesti painottanut salaisen tiedonhankinnan yhteydessä (PeVL 32/2013, s. 4 ja 33/2013, s. 4).

15 Tiedustelumenetelmän käytöstä ilmoittaminen ja raportointi

Electronic Frontier Finland – Effi ry katsoo, että tiedustelun kohteelle ilmoittamista koskevat säännöset ovat ristiriidassa Euroopan ihmisoikeustuomioistuimen (EIT) oikeuskäytännön kanssa. Tiedustelun kohteella oltava tosiasiallinen mahdollisuus viedä asia oikeuden tutkittavaksi (HE 202/2017 vp, s. 258–259). Mahdollisuutta ei ole, jos tiedustelun kohteeksi joutumisesta ei ilmoiteta. Ei ole väliä aloitetaanko asiassa rikostutkintaa, kun yksityisyyteen puuttuminen on joka tapauksessa tapahtunut. **Suomen journalistiliitto** katsoo olevan epäselvää, miten yksilön oikeusturva voidaan taata, jos tietoliikennetiedustelun kohteeksi päätymisestä ei aina edes tarvitse ilmoittaa.

Sisäministeriön vastaus: Sisäministeriö toteaa, että salaisen tiedonhankinnan kohteelle ilmoittamista koskevaa sääntelyä muutettiin viimeksi esitutkinta-, pakkokeino- ja poliisilain kokonaisuudistuksen yhteydessä (PolL 5:58 ja PKL 10:60). Poliisilain 5 luvun 58 §:n 1 momentin (1. virkkeen) mukaan telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, televalvonnasta, suunnitelmallisesta tarkkailusta, peittelystä tiedonhankinnasta, teknisestä tarkkailusta ja valvotusta läpilaskusta on viipymättä ilmoitettava tiedonhankinnan kohteelle kirjallisesti sen jälkeen, kun tiedonhankinnan tarkoitus on saavutettu (pääsääntö). Pykälän 2 momentissa säädetään poikkeuksista ilmoitusvelvollisuuteen. Tuomioistuin voi pidättämiseen oikeutetun poliisimiehen vaatimuksesta päättää, että 1 momentissa tarkoitettua ilmoitusta tiedonhankinnan kohteelle saadaan lykätä enintään kaksi vuotta kerrallaan, jos se on perusteltua käynnissä olevan tiedonhankinnan turvaamiseksi, valtion turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Ilmoitus saadaan tuomioistuimen päätöksellä jättää kokonaan tekemättä, jos se on välttämätöntä valtion turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Ilmoittamatta jättäminen tulisi kyseeseen ainoastaan kahdessa jälkimmäisessä tapauksessa. Kynnys kokonaan ilmoittamatta jättämiselle on puolestaan korkea, mitä kuvattaisiin ilmauksella ”välttämätöntä”. Lisäksi ilmoittamatta jättäminen tulee kyseeseen silloin, kun tiedonhankinnan kohteen henkilöllisyys ei ole tiedossa.

Yhtä lailla kuin voimassa olevassa lainsäädännössä, niin ehdotettavan siviilitiedustelulainsäädännön mukaan tuomioistuin voisi suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta päättää, että tiedustelumenetelmästä tehtävää ilmoitusta tiedonhankinnan kohteelle saadaan lykätä enintään kaksi vuotta kerrallaan, jos se on perusteltua käynnissä olevan tiedustelumenetelmän käytön turvaamiseksi, kansallisen turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Ilmoitus saataisiin tuomioistuimen päätöksellä jättää kokonaan tekemättä, jos se on välttämätöntä kansallisen turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi.

Tietoliikennetiedustelun käytöstä ilmoittamista koskisi edellä kerrotusta poiketen hieman erilainen ilmoituskonstruktio, josta ehdotetaan säädettäväksi tietoliikennetiedustelulakiehdotuksen 20 §:ssä. Pykälän mukaan jos 6 §:ssä tarkoitettua käsittelyssä on manuaalisesti selvitetty Suomessa olevan henkilön luottamuksellisen viestin tai tallentaman tiedon sisältö, ilmoitetaan hänelle tietoliikennetiedustelusta noudattaen, mitä poliisilain 5 a luvun 47 §:ssä säädetään telekuuntelusta ilmoittamisesta. Velvollisuutta ilmoittaa tietoliikennetiedustelusta ei kuitenkaan ole, jos tieto on hävitetty 9 §:n 2 momentin tai 15 §:n perusteella.

Edellä kerrotun perusteella velvollisuutta ilmoittaa tietoliikennetiedustelusta sen kohteelle ei olisi silloin, kun tietoliikennetiedustelusta on päätetty kiiretilanteessa ja tuomioistuin katsoo, ettei edellytyksiä tietoliikennetiedustelulle ole ollut. Tuomioistuimen päätöksen perusteella

tietoliikennetiedustelun käyttö lopetettava välittömästi sekä sillä saatu aineisto ja sillä saatuja tietoja koskevat muistiinpanot heti hävitettävä. Lisäksi, jos tietoliikennetiedustelulla saadut tiedot koskevat tietoja, jotka on hävitetty sen takia, että 1) viestinnän molemmat osapuolet olivat Suomessa silloin, kun viestintä tapahtui; 2) lähettäjällä tai vastaanottajalla taikka tallentajalla on velvollisuus tai oikeus kieltäytyä todistamasta kyseisestä tiedosta 12 §:ssä tarkoitetulla tavalla; 3) tietoa ei tarvita kansallisen turvallisuuden suojaamiseksi, niin tietoliikennetiedustelusta ei olisi velvollisuutta ilmoittaa tietoliikennetiedustelusta sen kohteelle.

Euroopan ihmisoikeustuomioistuin on lukuisissa ratkaisuisaan ottanut kantaa kysymykseen siitä, tuleeko ja missä tilanteissa tiedonhankinnan kohdehenkilöllä olla oikeus saada viranomaiselta tieto häneen kohdistetusta tiedonhankintatoimenpiteestä, esimerkiksi tietoliikennetiedustelusta. Kesäkuussa annetussa *Centrum för Rättvisa v. Ruotsi* –ratkaisussa EIT katsoi, että tiedustelutoiminnan luonne huomioon ottaen aina ei voida pitää mahdollisena sitä, että tiedustelutoimivaltuuden käytöstä ilmoitetaan sen kohteelle välittömästi käytön jälkeen, sillä se saattaisi vaarantaa koko tiedustelutoiminnan pitkän aikavälin tarkoituksen. Ilmoittamatta jättämisestä ei voida yksinään vetää johtopäätöstä, ettei tiedustelutoiminta silti olisi ollut välttämätöntä demokraattisessa yhteiskunnassa. Ilmoitusvelvollisuuden ei tarvitse olla absoluuttinen, jos ilmoitusvelvollisuuden rajoituksille on olemassa muita ilmoitusvelvollisuutta kompensoivia keinoja. Tällainen ilmoitus tulisi kuitenkin tehdä niin pian kuin mahdollista silloin kun se ei voi enää vaarantaa alkuperäisen rajoituksen tarkoitusta.

EIT on myös aiemmassa ratkaisukäytännössään korostanut, että tiedonhankinnan kohdehenkilöllä on oltava käytössään tehokkaat oikeusturvakeinot mahdollisesti lainvastaista viranomaistiedonhankintaa vastaan. Valitus- tai kantelumahdollisuuden käytön edellytyksenä on ihmisoikeustuomioistuimen toteamalla tavalla yleensä se, että henkilö saa viranomaiselta tiedon häneen kohdistetusta salaisesta tiedonhankinnasta sen jälkeen kun salaisen tiedonhankintamenetelmän käyttö on päättynyt. EIT:n ratkaisukäytännön mukaan tästä ei kuitenkaan seuraa, että ilmoitus on tehtävä välittömästi tiedonhankinnan päätyttyä. Uhka, josta tiedonhankintamenetelmän avulla on hankittu tietoja, voi jatkua vuosia tai jopa vuosikymmeniä, jolloin ilmoituksen tekemistä on turvallisuusviranomaisten toiminnan suojaamiseksi välttämätöntä lykätä vastaavasti. Oikeussuojakeinon käytön mahdollistamiseksi ilmoitus olisi kuitenkin tehtävä sen jälkeen, kun ilmoittamatta jättämiselle ei enää ole yksilöllistä perustetta. Kuitenkin myös järjestelmä, joka ei edellytä kohdehenkilölle ilmoittamista, voi olla sopusoinnussa ihmisoikeussopimuksen kanssa. Tällöin oikeus kannella viranomaisen salaisesta tiedonhankinnasta on tullut kansallisessa lainsäädännössä säättää sillä tavalla yleiseksi, että kuka hyvänsä saa kannella pelkästään sen perusteella, että epäilee viranomaisen saattaneen puuttua luottamuksellisen viestintänsä nauttimaan suojaan (*EIT Kennedy v. Yhdistynyt Kuningaskunta*).

Tiedustelutoimintaa varten ehdotetaan perustettavaksi oma laillisuusvalvontaa suorittava viranomainen, Tiedusteluvaltuutettu, joka olisi riippumaton ja sillä olisi laajat tiedonsaantioikeudet sekä viime kädessä mahdollisuus keskeyttää tiedustelumenetelmän käyttö. Useimmissa Euroopan maissa on parlamentaarisen valvontaelimen ohella erillinen tiedustelutoiminnan laillisuusvalvontaa harjoittava taho. Tiedusteluvaltuutettu toimisi tietosuojavaltuutetun toimiston yhteydessä ja olisi toiminnassaan itsenäinen ja riippumaton. Tiedusteluvaltuutetun tehtävänä olisi valvoa tiedustelumenetelmien käytön lainmukaisuutta sekä perus- ja ihmisoikeuksien toteutumista tiedustelutoiminnassa. Yksilöt voisivat tehdä tiedusteluvaltuutetulle kanteluita tiedustelutoiminnan laillisuuskysymyksistä. Lisäksi tiedustelutoiminnan kohteena ollut tai henkilö, joka epäilee, että häneen on kohdistettu tiedustelua, voisi pyytää valtuutettua tutkimaan häneen kohdistuneen toiminnan lainmukaisuuden. Valtuutettu voisi tehdä tarkastuksia tiedustelutoiminnan laillisuuden valvomiseksi, minkä lisäksi sille ehdotetaan oikeutta päästä valvonnan kannalta välttämättömiin tiloihin ja tietojärjestelmiin. Tiedusteluvaltuutettu voisi lisäksi määrätä tiedustelumenetelmän käytön keskeytettäväksi tai lopetettavaksi, jos hän katsoo valvottavan menetelleen lainvastaisesti tiedustelutoiminnassa.

Tiedusteluvaltuutettu harjoittaisi tiedustelutoiminnan kattavaa ja reaaliaikaista valvontaa. Tiedustelutoiminnan valvonnasta annettavassa laissa säädettäisiin valtuutetun oikeudesta olla läsnä tiedustelumenetelmää koskevan lupa-asian tuomioistuinkäsittelyssä. Siviilitiedustelulainsäädännössä tiedusteluviranomaisille säädettäisiin puolestaan velvollisuus ilmoittaa valtuutetulle tiedustelumenetelmän käytön viranomais- ja tuomioistuinpäätöksistä.

Sisäministeriö katsoo mm. edellä kerrotuilla perusteilla, että siviilitiedustelua koskeva hallituksen esitys on EIT:n ratkaisukäytännön mukainen ja sopusoinnussa Euroopan ihmisoikeussopimuksen kanssa.

Effi ry ja **VTT** ovat esittäneet, että tiedustelutoiminnasta tulisi kertoa mahdollisimman avoimesti. Lausunnoissa on esitetty, että julkisissa esityksissä voitaisiin ilmoittaa määrällisiä tietoja muun muassa tietoliikennetiedustelun osalta, kuinka laajoihin henkilöryhmiin, kuinka isoon verkkoalueeseen ja data- ja viestimääriin myönnetyt tiedusteluluvat ja toisaalta toteutetut tiedustelutoimenpiteet ovat kohdistuneet. Lisäksi lausunnoissa esitetään, että julkisiin esityksiin voitaisiin lisätä tilastoja siitä, paljonko ja kuin monta eri henkilöä koskevia tietoja tiedusteluviranomaiset ovat saaneet muiden viranomaisten rekistereistä.

Sisäministeriön vastaus: Tiedustelutoiminnan yhteiskunnallisen hyväksyttävyyden näkökulmasta lausunnoissa esitettyä voidaan pitää lähtökohtaisesti kannatettavana ja mahdollisuuksien mukaan salassapitosäännökset huomioon ottaen toiminnasta voitaneen laatia myös julkisia lausunnossa tarkoitettuja tilastoja. Siviilitiedustelun tehtävänä on hankkia ennakoivaa ja merkityksellistä tietoa kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. Tiedonhankinnan tehokkuutta ei tällöin voida perustellusti arvioida määrällisten, vaan laadullisten kysymysten kautta. Määrällinen mittari voi olla jopa harhaanjohtava. Pelkästään tiedustelukysymykseen tietoa hankkiva toimeksianto voi olla vähempimerkityksellinen kuin tiedusteluoperaatio, jossa vain osa hankitusta tiedosta kuuluu tiedustelukysymykseen.

Kattavin kuva edellä tarkoitetuista tiedoista koko tiedustelutoiminnassa, siviili- ja sotilastiedustelussa, olisi tiedusteluvaltuutetulla. Julkaistavat tiedot ja tilastot tulee kuitenkin käydä tarkasti läpi tiedusteluviranomaisten ja tiedusteluvaltuutetun kanssa, jottei tiedustelun tarkoitus vaarannu. Päätös tietojen julkistamisesta tulisi olla aina viime kädessä tiedusteluviranomaisella.

16 Yrityssalaisuuden suoja

Elinkeinoelämän keskusliitto EK ry, Suomen puolustus- ja ilmailuteollisuusyhdistys PIA ja Suomen Internet-yhdistys SIY ry ja Google kiinnittävät lausunnoissaan huomiota yrityssalaisuuden suojaan. EK pitää esitystä hyvänä, mutta muistuttaa, että yrityssalaisuuksia koskevasta tiedonluovutusrajoituksesta olisi perusteltua säätää perustelujen sijaan pykälätasolla. Google esittää huolensa siitä, ettei lakiehdotus aseta rajoituksia sille, minkälaista tietoa tiedusteluviranomainen saa ilmaista muille toimijoille. Ongelmallista on myös se, ettei ole olemassa ulkopuolista tahoa, joka valvoisi, minkälaista tietoa tiedusteluviranomainen ilmaisee muille yksittäisille toimijoille. Google katsoo, että kaikkeen lainsäädäntöön tulisi sisällyttää yleinen pääsääntö, jossa tällainen tietojen ilmaiseminen kielletään.

Sisäministeriön vastaus: Lausunnonantajien huomiot koskien yrityssalaisuuden suojaa ovat perusteltuja.

Suojelupoliisin oikeudesta luovuttaa tietoja ehdotetaan säädettäväksi muun muassa poliisilain muuttamista koskevan poliisilakiehdotuksen 5 a luvun 55 §:ssä (Yhteistyö muiden viranomaisten ja yhteisöjen kanssa) ja 57 §:ssä (Kansainvälinen yhteistyö) sekä tietoliikennetiedustelulakiehdotuksen 16 §:ssä (Haitallista tietokoneohjelmaa tai -käskyä koskevien tietojen luovuttaminen viranomaiselle, yritykselle tai yhteisölle). Muita paitsi kansainvälistä yhteistyötä koskevia säännösehdotuksia on käsitelty aiemmissa vastauksissa.

Kansainvälistä yhteistyötä koskevan 57 §:n 2 momentin mukaan suojelupoliisi voisi salassapitosäännösten estämättä luovuttaa tietoja kansainvälisessä yhteistyössä, jos tietojen luovuttaminen on tarpeen kansallisen turvallisuuden suojaamiseksi eikä tietojen luovuttaminen ole vastoin kansallista etua. Tietojen luovuttaminen kansainvälisessä yhteistyössä tulisi ensinnäkin perustua suojelupoliisin tehtävään suojata kansallista turvallisuutta. Käytännössä kyse voisi olla tiedustelumenetelmien tekniikkaa ja taktiikkaa, haittaohjelmia koskevista tiedoista tai turvallisuusuhkia koskevista analyyseistä taikka muusta sellaisesta tiedosta, jonka luovuttaminen olisi Suomen intressien mukaista. Tiedon luovuttamisen tulee toisaalta aina olla kansallisen edun mukaista. Tällaisen edun piiriin kuuluvat esimerkiksi tiedot Suomen poliittisista tai taloudellisista suhteista toisen valtion kanssa, sotilastiedustelua tai sotilaallista maanpuolustusta koskevat tiedot taikka tiedot kansainvälisen tiedusteluyhteistyön turvaamiseksi. Tietojen luovuttamisen hyväksyttävyyttä tulisi näin ollen arvioida yhtäältä kansallisen turvallisuuden suojaamisintressin ja toisaalta kansallisten etujen turvaamisintressin kannalta. Tässä kokonaisarvioinnissa suojelupoliisin on otettava huomioon myös luovutettavan tiedon ominaisuudet sekä tiedon vastaanottajana oleva taho.

17 Ilmiantajan suoja (ns. whistleblower)

Effi ry, Ihmisoikeusliitto ja Amnesty International Suomen osasto ovat kiinnittäneet huomiota siihen, että henkilöitä, jotka ilmoittavat tiedustelutoiminnassa tehtyjä loukkauksia, tulisi suojella rikosoikeudellisilta seuraamuksilta. **Effi ry** ehdottaa lainsäädäntöön ns. Whistleblower-suojaa. EU:n tietosuojasetuksen kansallista toimeenpanoa koskevassa TATTI-mietinnössä (Oikeusministeriön julkaisu 35/2017) on ehdotettu uuteen tietosuojalakiin 20 §:ää, jossa säädettäisiin väärinkäytöksen ilmoittaneen tahon henkilöllisyyden suojaamisesta. Vastaava sääntely tulisi omaksua tiedustelulainsäädäntöön.

Sisäministeriön vastaus: Lausunnonantajien huomiot ovat perusteltuja, mutta erityisiä säännöksiä ilmoittajan suojaksi ei ole tarpeen säätää. Jos henkilö havaitsee tiedusteluviranomaisen sisällä lainvastaisen menettelyn tai jos tiedusteluviranomaisen toiminta rikkoisi perus- ja ihmisoikeuksia eikä esimiehet tai sisäinen oikeudellinen valvonta tai sisäministeriön oikeudellinen valvonta olisi puuttunut tähän, niin henkilö voisi kääntyä tiedusteluviranomaisen, oikeuskanslerin tai eduskunnan oikeusasiamiehen puoleen. Tiedusteluvaltuutetulle tehtävä kanteluoikeus olisi yleinen eli kantelun voisi tehdä asianosainen tai kuka tahansa muu henkilö. Kantelun voisi tehdä myös oikeushenkilö. Kantelumenettely täydentäisi tiedusteluvaltuutetun oma-aloitteista toimintaa kattavan laillisuusvalvonnan takaamiseksi sekä turvaisi sen, että yksilöt pääsevät oikeuksiinsa ja että oikeusturvajärjestelmä toimii moitteettomasti. Käytännössä kantelun voisi tehdä myös anonyymina ja tiedusteluvaltuutettu voisi kantelun perusteella ottaa asian oma-aloitteisesti tutkittavaksi. Tämä mahdollisuus on olemassa nykyisin ylimpien laillisuusvalvojen kohdalla ja he voivat ottaa asian käsiteltäväkseen myös omasta aloitteestaan, jolloin ilmoittajan aloitteesta käynnistettyihin toimiin ryhtymisessä olisi mahdollista menetellä niin, ettei ilmoittajan henkilöllisyys tulisi julki.

18 Henkilötietojen käsittely

Liikenne- ja viestintäministeriö katsoo lausunnossaan, että: "Tiedusteluviranomaisille on esityksessä ehdotettu uutta tietoliikennetiedustelua koskevaa toimivaltuutta. Tietoliikennetiedustelusta on tekniseltä toteuttamistavaltaan sen kaltaista, että sen puitteissa tiedusteluviranomainen voisi saada teknisen mahdollisuuden seuloa myös hyvin monen suomalaisen luottamuksellista viestintää. Tämän vuoksi on erityisen tärkeää huolehtia riittävästä perusoikeuksien suojasta. Perusoikeussuojan toteutumisen kannalta laissa on keskeistä säätää riittävästä vaatimuksista tiedustelun kohdentamiselle sekä tiedustelumenetelmällä kerätyn luottamuksellisen viestin salaisuuden suojan alaisen tiedon käsittelylle. Lisäksi on huolehdittava siitä, että tiedustelu voidaan tosiasiallisesti teknisesti toteuttaa laissa säädettyjen perusoikeuksien suojaavien vaatimusten mukaisesti."

Tietosuojavaltuutetun toimisto toteaa, että nyt käsiteltävänä oleviin hallituksen esityksiin ei sisälly ehdotuksia valmisteilla oleviksi laeiksi henkilötietojen käsittelystä poliisitoimissa. Taustalla on puolestaan mm. Euroopan unionin tietosuojadirektiivistä (2016/680) aiheutuva implementointitarve. Näin ollen pelkästään nyt käsiteltävänä olevien hallitusten esitysten pohjalta ei ole mahdollista saada kokonaiskuvaa ko. viranomaisten henkilötietojen käsittelystä. Myös **Electronic Frontier Finland – Effi ry** on kiinnittänyt huomiota tietojen käsittelyyn kansainvälisessä yhteistyössä.

Sisäministeriön vastaus: Sisäministeriö yhtyy liikenne- ja viestintäministeriön näkemykseen perusoikeuksien suojan riittävästä turvaamisesta. Sisäministeriö katsoo, että perusoikeussuojan toteutumisen kannalta lakiehdotuksissa esitetään säädettäväksi riittävästä vaatimuksista tiedustelun kohdentamiselle. Siviilitiedustelulainsäädännön yhteydessä ehdotetaan henkilötietojen käsittelystä poliisitoimissa annettua lakia muutettavaksi ainoastaan välttämättömiltä osilta, koska poliisin pä koskevan lainsäädännön kokonaisuudistus on käynnissä. Esityksellä uudistetaan voimassa oleva henkilötietojen käsittelystä poliisitoimissa annettu laki poliisitoiminnan tarpeet huomioon ottaen. Säännöksissä huomioidaan Euroopan unionin tietosuojalainsäädännön vaatimukset. Kyseisen hankkeen on tarkoitus edetä eduskuntaan kuluvan vuoden aikana. Henkilötietojen käsittelystä säädetään siis tässä yhteydessä, kun siviilitiedustelulainsäädännön kohdalla kyse on pääsääntöisesti muiden tietojen käsittelystä.

19 Virkamiesten koulutus

KKO katsoo, että ehdotetun lainsäädännön mukaisia lupa-asioita käsitteleville tuomareille tulisi järjestää riittävästi koulutusta, jossa käsitellään avoimesti ja konkreettisesti tiedustelutoimintaa ja -menetelmiä. Tuomareita tulisi perehdyttää myös tiedustelumenetelmien käyttöön liittyviin perus- ja

ihmisoikeuskysymyksiin, kuten asiaa koskevaan Euroopan ihmisoikeustuomioistuimen tulkintakäytäntöön. Yksi tapa syventää tuomareiden asiantuntemusta olisi pyrkiä järjestämään vierailuja, yhteisiä seminaareja tai muita tilaisuuksia, joissa suomalaiset tuomarit voivat vaihtaa kokemuksia sellaisten ulkomaisten tuomareiden kanssa, joilla on kokemusta vastaavanlaisen tiedustelulainsäädännön soveltamisesta.

Professori Olli Mäenpää toteaa, että ehdotettuja toimivaltuuksia on joka tapauksessa käytettävä erityisesti luottamuksellisen viestin suojan perus- ja ihmisoikeussuoja huomioon ottaen. Tämä edellyttää tiedusteluvirkamiesten asianmukaista ja riittävää koulutusta sekä suojelupoliisin sisäisen ohjauksen ja valvonnan riittävyttä.

Suomen lakimiesliitto toteaa lausunnossaan, että lupa-asioiden käsittelyyn tulee kiinnittää erityistä huomiota mm. koulutusta lisäämällä, koska uusilla tiedustelumenetelmillä puututtaisiin merkittävällä tavalla yksilön perus- ja ihmisoikeuksiin.

Sisäministeriön vastaus: Uusien tiedustelutoimivaltuuksien riittävä hyödyntäminen ja sitä kautta saavutettava yhteiskunnallinen vaikuttavuus ulko- ja turvallisuuspoliittisessa päätöksenteossa, oikea-aikaisessa turvallisuustilannekuvassa viranomaisille ja kansantaloudellisten etujen suojaamisessa edellyttää resursoinnin oikea-aikaisuutta. Resursointi, koulutus ja toiminnan suunnittelu tulisi siksi käynnistää riittävän aikaisessa vaiheessa jo ennen lainsäädännön voimaantuloa.

Suojelupoliisi ei voisi jatkossa nojautua yksinomaan Poliisiammattikorkeakoulun ja keskusrikospoliisin suunnittelemiin ja järjestämiin koulutuksiin salaisen tiedonhankinnan osalta, koska siviilitiedustelussa käytettävien toimivaltuuksien käyttöperuste, käyttöön liittyvät taktiset näkökohdat, kokonaan uudet toimivaltuudet ja menetelmien henkilöllinen kohdentaminen eroavat perinteisistä rikostorjuntamenetelmistä. Lisäksi menetelmiä on määrä käyttää uudessa toimintaympäristössä eli ulkomailla. Uusien siviilitiedustelutoimivaltuuksien koulutusrakenteet olisi siten luotava ja vakiinnutettava viraston sisälle. Tarkoitus on perustaa suojelupoliisiin koulutusyksikkö, joka vastaisi viraston henkilöstön erikois- ja jatkokoulutuksesta ja siviilitiedustelulain edellyttämästä päällystön erikoiskoulutuksesta sekä osallistuisi sotilastiedusteluviranomaisen, tuomioistuimien ja laillisuusvalvonnan kanssa tehtävään koulutusyhteistyöhön. Tässä vaiheessa suojelupoliisi arvioi, että suojelupoliisin koulutustoiminto sisältäisi perehdytysvaiheessa 6 henkilötyövuotta, joista 2 määräaikaista ja ylläpitovaiheessa 4 pysyvää henkilötyövuotta. Osa taktisesta koulutuksesta olisi hankittava sellaisilta kansainvälisiltä yhteistyötahoilta, joilla on pitkäaikainen kokemus tiedustelutoimivaltuuksien käytöstä. Lainsäädäntömuutoksista aiheutuva organisaation henkilömäärän kasvu edellyttäisi myös henkilöstöhallintoon sekä viraston talous- ja yleishallintoon liittyvien resurssien pysyvää vahvistamista.

Suojelupoliisissa ei ole nykyisin päätoimista sisäistä laillisuusvalvontatoimintoa, vaan sisäistä laillisuusvalvontaa suoritetaan samoin kuin muussakin poliisissa sivutoimisesti ja pääasiassa määräaikaisten tarkastusten muodossa.

Uusien tiedustelutoimivaltuuksien myötä viraston sisäisen laillisuusvalvonnan merkitys korostuu. Sisäinen laillisuusvalvonta olisi järjestettävä entistä reaaliaikaisemmaksi, tehokkaammaksi ja kattavammaksi, mikä edellyttäisi eriyttämistä omaksi toiminnokseen ja siten lisäresursseja (4htv). Samalla olisi järjestettävä sisäisen laillisuusvalvonnan suhde ulkoisiin laillisuusvalvontaelimiin, ennen kaikkea tähän esitykseen liittyvässä oikeusministeriön esityksessä ehdotettavaan valvontaviranomaiseen. Laillisuusvalvonta tekisi tiivistä yhteistyötä koulutusyksikön kanssa oikeiden soveltamiskäytäntöjen jakamiseksi tiedustelutoimivaltuuksia käyttäville virkamiehille. Sisäisen laillisuusvalvonnan järjestäminen edellyttäisi osin rahoitusta jo ennen lain voimaantuloa siten, että toimintoa varten suojelupoliisiin tarvitsemasta arvioidusta kokonaishenkilöresurssista 3 henkilötyövuotta saataisiin käyttöön vuosi ennen lain voimaantuloa. Tämä mahdollistaisi sen, että oikeisiin soveltamiskäytäntöihin perustuva riittävästi koulutettu siviilitiedustelumenetelmien käyttö voitaisiin aloittaa täysimittaisesti heti lain voimaantullessa.

Lisäksi operatiivisiin yksiköihin perustetaan kaksi uutta operatiivisen lakimiehen miehen virkaa, joilla tuetaan uusien kotimaan, ulkomaan ja tietoliikennetiedustelutoimivaltuuksien operatiivista tiedonhankintaa. Nämä virat sisältyvät sisäisen laillisuusvalvonnan kokonaisresurssitarpeeseen 4 henkilötyövuotta. Edellä kuvatulla jaolla varmistetaan, että laillisuusvalvonta ja operatiivinen päätöksenteko pidetään jatkossakin erillään.

Lupa-asioita käsitteleville tuomareille on tarpeen myös järjestää riittävästi koulutusta, jossa käsitellään avoimesti ja konkreettisesti tiedustelutoimintaa ja -menetelmiä. Tuomareita on tarpeen perehdyttää

myös tiedustelumenetelmien käyttöön liittyviin perus- ja ihmisoikeuskysymyksiin, kuten asiaa koskevaan Euroopan ihmisoikeustuomioistuimen tulkintakäytäntöön.

20 Tuomioistuinmenettely

Helsingin käräjäoikeus toteaa, ettei esityksen perusteluista käy ilmi, että tiedusteluviranomaisen on toimitettava tieto lupahakemuksesta tiedusteluvaltuutetulle. Epäselväksi sen sijaan jää, kuka ilmoittaa tiedusteluvaltuutetulle istunnon tarkasta ajankohdasta ja paikasta. Käräjäoikeus katsoo, että viimeksi mainittu ilmoitusvelvollisuus tulisi asettaa tiedusteluviranomaiselle.

Sisäministeriön vastaus: Helsingin käräjäoikeuden huomio on hyvä. Lupahakemuksen toimittamisen tekemistapaa pohdittiin lakien valmistelun aikana ja erilaisia käytäntöjä myös esitettiin. Tiedusteluvaltuutetulla läsnäolo-oikeus käsiteltäessä tiedustelumenetelmää koskevaa lupa-asiaa tuomioistuimessa ei tosiasiaassa toteudu, jos hän ei saa ilmoitusta lupa-asiaa koskevasta käsittelystä. Tämä on kuitenkin eri asia kuin lupahakemuksen toimittaminen ennen käsittelyä.

Tiedusteluvaltuutetulle ehdotetaan säädettäväksi läsnäolo-oikeudesta, ei läsnäolovelvollisuudesta tuomioistuinkäsittelyssä. Läsnäolo-oikeuden käyttäminen olisi tiedusteluvaltuutetun itsenäisessä harkinnassa ja hän voisi itse ratkaista, pitääkö läsnäoloaan tarpeellisenä. Tiedustelutoiminnan valvontalakiehdotuksen yksityiskohtaisissa perusteluissa todetaan, että tiedusteluviranomaisen olisi toimitettava tieto tuomioistuimelle toimitetusta lupahakemuksesta yhteisen tietojärjestelmän kautta tai muulla tavalla siten, että valtuutetulla olisi mahdollisuus varautua osallistumaan tuomioistuimen kyseiseen istuntoon. Läsnäolo-oikeus tulisi turvatuksi valtuutetulle tuomioistuinkäsittelystä kohtuullisessa ajassa tehtävällä ilmoituksella (HE 199/2018 vp., s. 58).

Vaikka ilmoituksen tekijää ja lupahakemuksen toimittamista koskevat oikeusohjeet löytyvät tiedustelutoiminnan valvontaa koskevan lakiesityksen perusteluista, mutta oikeuslähdearvon sekä informatiivisuuden parantamiseksi voi olla tarpeen säätää kyseisistä asioista laintasolla. Jos eduskunta katsoo Helsingin käräjäoikeuden huomion aiheelliseksi, niin poliisilakiehdotuksen 5 a luvun 35 §:ään voitaisiin muuttaa lisäämällä siihen uusi 8 momentti.

Tiedustelumenetelmän käyttöä koskeva vaatimus on viipymättä annettava tiedoksi tiedusteluvaltuutetulle. Samalla on ilmoitettava tiedustelumenetelmän lupa-asian käsittelyn ajankohta, jos se on tiedossa.

Sisäministeriön vastaus: Lupa-asioita käsitteleville tuomareille tullaan järjestämään riittävästi koulutusta, jossa käsitellään avoimesti ja konkreettisesti tiedustelutoimintaa ja -menetelmiä. Tuomareita tullaan myös perehdyttämään koulutuksessa tiedustelumenetelmien käyttöön liittyviin perus- ja ihmisoikeuskysymyksiin, kuten asiaa koskevaan Euroopan ihmisoikeustuomioistuimen tulkintakäytäntöön.

Tiedustelumenetelmien käytöstä ja ns. uhkaperusteisesta tiedonhankinnasta ei Suomessa ole olemassa oikeuskäytäntöä tai säädösperustan historiaa. Siviilitiedustelun kohteet ja vakava uhka kansalliselle turvallisuudelle eivät myöskään perustu rikoslain tavalla eksakteihin tunnusmerkistöihin. Muun muassa näistä syistä tiedusteluviranomaisen tulee esittää tuomioistuimelle vakuuttava näyttö ja muu selvitys, että kuka tahansa huolellisesti asioita harkitseva henkilö voisi päätyä tuomioistuimen kanssa luvan myöntävään ratkaisuun. Tuomioistuin voi myös aktiivista kyselyoikeuttaan käyttämällä varmistua sille esitettyjen seikkojen riittävydestä ja selkeydestä

Siviili- ja sotilastiedustelumenetelmien lupakäsittelyä Helsingin käräjäoikeudessa ja toimenpiteen kohteen oikeusturvaa on valvomassa myös tiedusteluvaltuutettu. Valtuutetun oikeudellinen valvonta kohdistuisi nimenomaan tiedusteluviranomaiseen, ei tuomioistuimen toimintaan. Läsnäolo-oikeudella turvattaisiin tiedusteluvaltuutetun mahdollisuus saada tietoonsa reaaliaikaisesti kaikki tuomioistuinkäsittelyssä esillä olevat seikat tiedustelumenetelmän käytön perusteista ja edellytyksistä. Käytännössä osa lupahakemuksen tueksi esitetyistä seikoista annetaan tuomioistuimelle suullisesti. Läsnäolo-oikeus myös ohjaisi osaltaan tiedusteluluvan hakijaa riittävien perustelujen esittämiseen tiedustelumenetelmän käyttölupahakemuksessa (HE 199/2017 vp., s. 58).

Tiedusteluvaltuutetun roolista ks. lausunnon kohta 7 Tiedusteluvaltuutetun rooli tuomioistuimessa.

21 Ilmaisukielto

Google toteaa, että ehdotetussa säännöksessä asetetaan vuoden mittainen määräaika, jonka kuluessa tiedustelun tiedonkeräystapoja koskevat tiedot voidaan määrätä salassa pidettäväksi niin, ettei kolmas osapuoli saa niitä ilmaista tai paljastaa. Kieltoa voidaan kuitenkin uudistaa mahdollisesti loputtomiin, eikä kolmas osapuoli tällöin voi valittaa tästä (Poliisilaki, 5a-luku, 38 §). Tarkoituksena on ymmärrettävästi suojella yksittäistapauksissa tiedustelutiedon keräystä ja käytettyjä tiedustelutapoja. Läpinäkyvyyden varmistamiseksi tulisi lainsäädännössä kuitenkin yksilöidä, ettei ilmaisukielto saisi kerrallaan kestää yli vuoden mittaista aikaa, jonka jälkeen viranomaisilla olisi mahdollisuus hakea yhtä vuoden mittaista pidennystä.

Sisäministeriön vastaus: Poliisilain muuttamista koskevan poliisilakiehdotuksen 5 a luvun 38 §:ssä ehdotetaan säädettäväksi ilmaisukiellosta siviilitiedustelussa. Pykälän 1 momentin mukaan tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies saa kieltää sivullista ilmaisemasta tämän tietoon tulleita seikkoja tiedustelumenetelmän käytöstä siviilitiedustelussa, jos se on perusteltua tiedustelumenetelmän käytön suojaamiseksi. Edellytyksenä on lisäksi, että sivullinen on tehtävänsä tai asemansa johdosta avustanut tai häntä on pyydetty avustamaan tiedustelumenetelmän käytössä.

Tiedustelumenetelmän käytön perusteena on aina, että siviilitiedustelun kohteena oleva toiminta vakavasti uhkaa kansallista turvallisuutta. Tiedustelumenetelmää käytettäessä on mahdollista joutua tilanteeseen, joissa ulkopuolinen apu on tarpeen tai jopa välttämätöntä. Esimerkiksi paikkatiedustelussa voi olla tarpeen pyytää taloyhtiön huollosta vastaavan yhtiön palveluksia. Näin ollen sivulliset voivat saada tietoja, joiden ilmaiseminen voi vaarantaa ainakin tiedustelumenetelmän käytön, mutta samalla muodostaa uhkan kansalliselle turvallisuudelle. Tarkoitus olisi minimoida riski tiedustelumenetelmän käytön paljastumisesta sekä suojata samalla myös salassa pidettäviä taktisia ja teknisiä menetelmiä ja viime kädessä kansallista turvallisuutta.

Pykälän 1 momentin 2 virkkeen mukaan edellytyksenä olisi lisäksi, että sivullinen on tehtävänsä tai asemansa johdosta avustanut tai häntä on pyydetty avustamaan tiedustelumenetelmän käytössä. Ilmaisukieltoa ei siten voitaisi antaa kenelle tahansa henkilölle, esimerkiksi taloyhtiön asukkaalle tai muulle sivulliselle, joka sattumalta havaitsee teknisen tarkkailun laitteen asennuksen.

Säännöksessä tiedustelumenetelmän käytöllä tarkoitettaisiin tiedustelumenetelmien käyttöä laajemmin, joka pitäisi esimerkiksi sisällään siviilitiedustelussa sekä sotilastiedustelussa käytettävien tiedustelumenetelmien käytön suojaamisen silloin, kun suojelupoliisi ja sotilastiedusteluviranomainen toimisivat yhteistyössä. Ilmaisukielto olisi perusteltua antaa ainakin silloin, jos tiedustelumenetelmän käyttö saattaisi paljastua ilman kiellon määräämistä sivulliselle.

Ilmaisukiellon saanut saisi ilman määräaikaa kannella päätöksestä. Kantelu olisi käsiteltävä kiireellisenä. Ilmaisukieltoa koskevasta päätöksestä tulisi myös aina ilmoittaa tiedusteluvaltuutetulle, joka arvioisi ilmaisukiellon oikeudelliset edellytykset ja tarvittaessa puuttuisi tiedusteluviranomaisen menettelyyn.

22 Vieraan valtion virkamies tiedustelumenetelmän käyttäjänä

Eduskunnan oikeusasiamies toteaa lausunnossaan, että ehdotuksen 57 §:n 3 momentissa todetaan, että vieraan valtion toimivaltaisella virkamiehellä on suojelupoliisin päällikön päätöksellä oikeus Suomen alueella kansallisen turvallisuuden suojaamiseksi toimia yhteistyössä suojelupoliisin kanssa ja suojelupoliisin poliisimiehen ohjauksessa ja valvonnassa käyttää niitä tiedustelumenetelmiä, joiden käytöstä päättämisestä säädetään 9, 10, 18, 20 ja 24 §:ssä. Näitä keinoja ovat suunnitelmallinen tarkkailu, peitelty tiedonhankinta, peitetoiminta, valeosto ja tietolähteen ohjattu käyttö. Oikeusasiamies pitää selvänä, että näiden tiedustelumenetelmien käyttö on perustuslain 124 §:ssä tarkoitettu julkinen hallintotehtävä, johon sisältyy julkisen vallan käyttöä, mahdollisesti merkittävää julkisen vallan käyttöä. Jos jonkun tiedustelumenetelmän, esimerkiksi peitetoiminnan, katsotaan sisältävän merkittävää julkisen vallan käyttöä, se voidaan PL 124 §:n mukaan antaa vain viranomaiselle, joka EOA:n käsityksen mukaan voi tarkoittaa vain suomalaista viranomaista. Joka tapauksessa tälle vieraan valtion virkamiehelle tulee PL 124 §:n vakiintuneen tulkintakäytännön mukaan säätää Suomen lain mukainen virka- ja vahingonkorvausvastuu.

Sisäministeriön vastaus: Poliisilakiehdotuksen 5 a luvun 57 §:ssä säädettäisiin kansainvälisestä yhteistyöstä. Pykälän mukaan suojelupoliisi voisi tehdä yhteistyötä sekä suorittaa yhteisiä operaatioita

ulkomaisten turvallisuus- ja tiedustelupalveluiden kanssa. Kansainvälisen avun antamista ja pyytämistä koskevasta päätöksenteosta säädetään erikseen siitä annetussa laissa 418/2017. Säännöksessä edellytettäisiin, että vieraan valtion virkamies olisi eräitä tiedustelumenetelmiä Suomessa käyttäessään velvollinen noudattamaan suojelupoliisin poliisimiehen antamia määräyksiä ja ohjeita. Tiedustelumenetelmien käyttö pysyisi näin ollen aina suomalaisen virkamiehen ohjauksessa ja valvonnassa. Selvää on lisäksi, että vieraan valtion virkamies olisi Suomessa toimiessaan rikos- ja vahingonkorvausoikeudellisen vastuun piirissä, jollei esimerkiksi hänen diplomaattiasemastaan muuta johtuisi. Näistä menettelytakeista ja vastuujärjestelyistä johtuen ehdotetun pykälän ei arvioida olevan ongelmallisessa suhteessa perustuslain 124 §:ssä säädettyyn vaatimukseen siitä, että merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan antaa vain viranomaiselle.

Pykälän 3 momentin 2. virkkeen mukaan vieraan valtion toimivaltaisella virkamiehellä olisi suojelupoliisin päällikön päätöksellä oikeus Suomen alueella kansallisen turvallisuuden suojaamiseksi toimia yhteistyössä suojelupoliisin kanssa ja suojelupoliisin poliisimiehen ohjauksessa ja valvonnassa käyttää niitä tiedustelumenetelmiä, joiden käytöstä päättämisestä säädetään 9, 10, 18, 20 ja 24 §:ssä. On syytä painottaa, että kansainvälisen yhteistyön lähtökohtana on aina Suomen kansallinen turvallisuus. Tiedustelumenetelmän käytön perusteet olisivat vastaavat kun suojelupoliisin itsenäisesti suorittamassa siviilitiedustelussa.

Kyseisen säännösehdotuksen yksityiskohtaisista perusteluista käy ilmi, että erityisesti tietoverkossa tapahtuvassa tarkkailussa voitaisiin tarvita toisen valtion sellaisen virkamiehen apua, jolla olisi suojelupoliisilta puuttuva ominaisuus tai osaaminen, kuten kielitaito tai kulttuurin tuntemus, jota suojelupoliisin virkamiehillä ei ole. Vastaavanlainen yhteisoperaation tarve voi liittyä peiteltyn tiedonhankintaan, peitetoimintaan, valeostoon ja tietolähteen ohjattuun käyttöön. Kyse olisi siitä, että vieraan valtion virkamies toimisi suojelupoliisin tiedonhankintaoperaatiossa avustavassa roolissa. Ulkomaisella virkamiehellä voi olla sellaista osaamista tai muita ominaisuuksia, joita suomalaisella virkamiehellä ei ole ja joita tarvittaisiin operaation onnistuneeksi toteuttamiseksi. Toisaalta vieraan valtion tiedustelupalvelun virkamiehellä saattaa olla sellaisia tietolähteitä, jotka ovat tarkoituksenmukaista kontaktoida suojelupoliisin kanssa ja tapaaminen tarkoituksenmukaista järjestää Suomessa.

23 Liitelait

23.1 Laki poliisin hallinnosta

Keskusrikospoliisi pitää hyvänä ja selkeänä sitä, että suojelupoliisilta poistetaan rikosten esitutkintavelvollisuus. Samalla kuitenkin todetaan, että nykyisin suojelupoliisin tutkittavaksi säädetty rikokset ovat siinä määrin vakavia ja tutkinnallisesti vaativia, että ne kuuluisivat luontevasti Keskusrikospoliisin tutkittavaksi. Keskusrikospoliisin näkemyksen mukaan asiasta voitaisiin säätää lain tasolla.

Sisäministeriön vastaus: Keskusrikospoliisin huomio on aiheellinen, koska suojelupoliisilta ehdotetaan poistettavaksi esitutkinta- ja pakkokeinotoimivaltuudet. Poliisin hallinnosta annetun lain (110/1992) 9 §:ssä säädetään keskusrikospoliisin tehtävistä eikä pykälää kuitenkaan ehdoteta tässä yhteydessä muutettavaksi.

24 Eräitä yhteensovittamisen tarpeita

24.1 Tietojenantovelvollisuus tietoliikennetiedustelussa

EK, FiCom, DNA, Elisa Oyj, Telia Oyj. Lausunnonantajat kiinnittävät huomiota tietoliikennetiedustelulain 22 §:n yksityiskohtaisiin perusteluihin, jotka olisi tarpeellista oikaista vastaamaan sotilastiedustelulain perusteluja. Pykälän tarkoittaman tiedonantovelvollisuuden piiriin kuuluvat tiedot koskisivat ennen kaikkea sitä, mitkä asiakasorganisaatiot ovat varanneet tiedonsiirtäjältä siirtokapasiteettia käyttöönsä ja mitä tiedonsiirtäjän hallitsemia rajan ylittävän viestintäverkon osia tällaiset varaukset koskevat. Pykälä velvoittaisi tiedonsiirtäjän antamaan tietoja myös muista mahdollisista seikoista, jotka vaikuttavat tietoliikenteen reitittymistodennäköisyyteen sen ylittäessä Suomen rajan tiedonsiirtäjän omistamassa tai sen hallinnassa olevassa viestintäverkon osassa. On syytä korostaa, että pykälä velvoittaisi tiedonsiirtäjän antamaan tietoja vain siltä kapasiteettia varanneista asiakasorganisaatioista, ei sen sijaan viestintätapahtumien osapuolena

olevista kuluttaja-asiakkaistaan. Pykälä ei muutenkaan perustaisi suojelupoliisille oikeutta hankkia tai saada tietoja yksittäisistä viestintätapahtumista tai niiden osapuolina olevista henkilöistä.

Sisäministeriön vastaus: Sisäasiainministeriö pitää lausunnonantajien muutosehdotusta kannatettavana. Yhdenmukaistamisvaatimus koskee alla olevaa perustelukohtaa. Myös siviilitiedustelua koskevan tietoliikennetiedustelulakiehdotuksen 22 §:n kohdalla pykälän tarkoittamat tietoliikennetiedustelun kohdentamiseksi välttämättömät tiedot koskisivat verkon teknistä toteuttamistapaa ja topologiaa esimerkiksi tietyn maantieteellisen alueen osalta. Pykälän mukaan tiedonsiirtäjää ei voitaisi velvoittaa luovuttamaan asiakkaana olevaa yksittäiseen luonnolliseen tai oikeushenkilöön liittyviä tietoja.

Siviilitiedustelulainsäädäntö	Sotilastiedustelulaki
L tietoliikennetiedustelusta siviilitiedustelussa <i>22 §:n perustelut (HE 202/2017 vp, s. 261)</i> Pykälän tarkoittaman tiedonantovelvollisuuden piiriin kuuluvat tiedot koskisivat ennen kaikkea sitä, mitkä asiakasorganisaatiot ovat varanneet tiedonsiirtäjältä siirtokapasiteettia käyttöönsä ja mitä tiedonsiirtäjän hallitsemia rajan ylittävän viestintäverkon osia tällaiset varaukset koskevat. Pykälä velvoittaisi tiedonsiirtäjän antamaan tietoja myös muista mahdollisista seikoista, jotka vaikuttavat tietoliikenteen reitittymistodennäköisyyteen sen ylittäessä Suomen rajan tiedonsiirtäjän omistamassa tai sen hallinnassa olevassa viestintäverkon osassa. On syytä korostaa, että pykälä velvoittaisi tiedonsiirtäjän antamaan tietoja vain siltä kapasiteettia varanneista asiakasorganisaatioista, ei sen sijaan viestintätapahtumien osapuolena olevista kuluttaja-asiakkaistaan. Pykälä ei muutenkaan perustaisi suojelupoliisille oikeutta hankkia tai saada tietoja yksittäisistä viestintätapahtumista tai niiden osapuolina olevista henkilöistä.	<i>95 §:n perustelut (HE 203/2017 vp, s. 328)</i> Pykälän tarkoittamat tietoliikennetiedustelun kohdentamiseksi välttämättömät tiedot koskisivat verkon teknistä toteuttamistapaa ja topologiaa esimerkiksi tietyn maantieteellisen alueen osalta. Pykälän mukaan tiedonsiirtäjää ei voitaisi velvoittaa luovuttamaan asiakkaana olevaa yksittäiseen luonnolliseen tai oikeushenkilöön liittyviä tietoja.

24.2 Tekninen laitetarkkailu

Rajapinta teknisen kuuntelun ja teknisen laitetarkkailun välillä määrittyy siviilitiedustelulaissa toisin kuin sotilastiedustelulaissa.

Siviilitiedustelulaissa viitataan teknisen kuuntelun ja teknisen laitetarkkailun määritelmien ja rajapintojen osalta niihin säännöksiin, jotka nykyisin sisältyvät poliisilain 5 lukuun ja pakkokeinolain 10 lukuun. Kyseisten säännösten mukaan teknisellä laitetarkkailulla ei saa hankkia tietoa viestin sisällöstä tai välitystiedoista. Sotilastiedustelulaki sisältää siviilitiedustelulaista poiketen teknisen laitetarkkailun omalajisen määritelmä- ja toimivaltuussäännöksen. Siinä missä siviilipuolen säännöksen mukaan teknisellä laitetarkkailulla ei saa hankkia tietoa viestin sisällöstä tai sen välitystiedoista, esitetään sotilastiedustelulaissa säädettäväksi, että teknisellä laitetarkkailulla ei saa hankkia tietoa *välitettävänä* olevasta viestistä tai sen välitystiedoista. Kielto on näennäinen, sillä se ainoastaan määrittää teknisen laitetarkkailun ja telekuuntelun välisen rajan, joka raja olisi olemassa ilman erillistä säännöstason mainintaakin. Kiellon käytännön merkitys on, että se sotilaspuolella siirtää kaiken näppäimistö- sekä hyöty-/haittaohjelman avulla tehtävän päätelaitteeseen kohdistuvan kuuntelun teknisen kuuntelun toimivaltuuden alaisuudesta teknisen laitetarkkailun toimivaltuuden alaisuuteen.

24.3 Tiedustelutoimivaltuuksien käyttö ulkomailla

Siviilitiedustelulain 39 §:ssä ehdotetaan säädettäväksi "tiedustelumenetelmien käytöstä päättämisestä eräissä tilanteissa" eli ulkomaantiedustelusta. Pykälän 3 momenttiin sisältyy luettelo niistä siviilitiedustelulain säännöksistä, joita ei tarvitse soveltaa ulkomaantiedustelun yhteydessä. Luettelosta puuttuu viittaus jäljentämiskieltoja koskevaan pykälään, mikä merkitsee sitä, että kyseiset kiellot tulisivat sovellettaviksi suojelupoliisin suorittaman ulkomaantiedustelun yhteydessä. Sotilastiedustelulain vastaavaan säännökseen sisältyy viittaus jäljentämiskieltoja koskevaan pykälään, mikä merkitsee sitä, että kyseiset kiellot eivät tulisi sovellettaviksi puolustusvoimien suorittaman ulkomaantiedustelun yhteydessä.

lainsäädäntöneuvos Marko Meriniemi